FORTRA

GUIDE (INFRASTRUCTURE PROTECTION)

How to Use Upskilling and Reskilling to Scale Your Cybersecurity Team

As security budgets get cut across the board, hard decisions must be made about what stays and goes. Offensive security (also referred to as “proactive security”) is one of the most effective ways for organizations to audit their security defenses, protect their networks, and stay compliant. Unfortunately, highly trained offensive security personnel are hard to come by. As the need for proactive security increases but the number of skilled professionals decreases, upskilling and reskilling are favored ways for organizations to scale their existing teams to meet demand. It all comes down to investing in your current staff and there are several benefits to doing this — for employer and employee.

The practice of upskilling and reskilling lets companies "hire" from within while giving employees the valuable training they need to be more indispensable in the workplace.

Upskilling and reskilling:

- Improve employee retention
- Create a growth environment for employees
- Are cost-effective ways to scale security teams, among other benefits

Offensive security measures — vulnerability management, pen testing, and red teaming — are critical to ensuring that an organization's security posture performs as needed when an adversary strikes. Giving current employees the chance to make a difference in the company through offensive security upskilling and reskilling is a wise, judicious use of resources at a time when resources are scarce.

What is Upskilling?

Upskilling teaches employees additional skills pertaining to their current role which would allow them to expand their present job capabilities and "do more."

Upskilling allows employees to build on their current skillsets and do more in their day. For example, a pen tester could get training to help perform occasional red team engagements as well, not only plumbing for known exploitable vulnerabilities but testing the infrastructure (and its defenses) with the latest adversarial tactics.

What is Reskilling?

Reskilling is teaching current employees new skills, in this case pertaining to cybersecurity, to enable them to make a career-switch to a more in-demand field. Not only does this save on new-hire overhead and leverage inter-departmental knowledge, but reskilling also improves the work culture and morale as employees are shown that their employers are willing to invest in them.

This could be the case of an IT administrator becoming a penetration tester, providing the IT admin with a whole new skill set. This could also constitute a wider career change, such as an accountant or healthcare professional training for a new role as a threat analyst.

Setting the Stage for the Reskilling Revolution

It's a story we all lived through but one that bears retelling. All organizations faced unprecedented digital change over the past ten years, with world events contributing to the accelerated pace. With every company now essentially a software company, a larger amount of software than ever needs to be protected.

Factor in every line of code written, every new application, burgeoning APIs, and the complete disintegration of the perimeter — not to mention breakneck cloud adoption rates and stunning AI advancements — and we begin to see why the limited cybersecurity teams of five years ago are struggling to bear up under the weight of new technologies, multiple steep learning curves, and ever-advancing adversarial techniques.

As the industry continues to persevere through a cyber talent crisis that promises to go nowhere, companies that were hoping to pay a premium for new talent are being blocked again by cybersecurity funding cuts across government and the private sector. Even venture capital firms aren't immune. This sets the stage for a looming question: How do organizations close the cyber talent gap? At a time when companies are being asked to make more bricks with less straw, creative and resourceful answers are in high demand. The solution to train existing employees to do cybersecurity-related tasks resonates with a lot of strapped organizations.

> *"Four million workers in the cybersecurity industry are needed worldwide."*
>
> **—2024 World Economic Forum**

Observes Bill Reynolds, research director at Foote Partners, a workforce research firm, "With the significant shortfall in the marketplace for skilled cybersecurity professionals, the sense I'm getting by talking to hundreds of employers … is that they're focusing more right now on training and developing talent from within."

Additionally, the World Economic Forum (WEF) suggests employers keep an open mind when it comes to hiring those with non-traditional cybersecurity skillsets and reskilling them. Notes the WEF, "It's a pivotal time to find job seekers interested in learning new skills or changing careers… But with the growing talent shortage, this recruiting approach must also be expanded to consider new talent pools and diverse expertise to help organizations fill unfilled positions."

The Benefits of Reskilling in Cybersecurity

As noted in CSO, "While the tendency is to seek out existing experts with technology-focused certifications or cyber-related degrees… an upskilling and reskilling strategy provides only an upside as organizations try to fill the cyber skills gap and keep their networks safe." Here are some of those upsides:

Benefits to the Employer

- **Cost Effective** — Given the wealth of knowledge contained in IT's shared skillset, many organizations are finding it far more favorable to train from within and spare the expense of recruiting, hiring, and training new employees. Additionally, a Gallup report estimated that replacing a current employee could cost twice their yearly salary.
- **Employee Retention** — It also helps keep the talent they already have; in a survey of Human Resources professionals, the Society of Human Resource Management (SHRM) found that 86% of respondents connected ongoing training to increased employee retention. And according to McKinsey, a major reason that employees quit is because they lacked opportunities to learn new things, which eventually made their work uninteresting or unchallenging.
- **Company Image** — From an employee's perspective, upskilling and reskilling indicate a willingness to invest in current talent, sends a message of loyalty, and, ironically, draws an ever-widening talent pool as the organization increasingly earns the image of a "best to work for" company. As noted in Forbes, "Upskilling improves an organization's reputation for supporting staff and their job satisfaction. This can provide a better company culture and external image of the brand, which in turn, makes it easier to attract and retain excellent employees."

Benefits to the Employee

- **Résumé Skills** — Without having to change companies or cultures, commutes or environments, workers can pad their resumes with in-demand skills and, in the case of cybersecurity careers, pad their paychecks as well.
- **Job Security** — In times of leanness, cybersecurity skills can be seen as insurance against layoffs in an economy where recession fears threaten to bring large job cuts in their wake. Employees with two valuable skillsets are much less likely to go, especially if one of them is cybersecurity.
- **Better work culture** — Upskilling benefits corporate culture in a number of ways. It increases morale, boosts productivity, contributes to a workforce that can adapt and stay agile, and creates an environment in which employees can grow both personally and professionally.
- **Job Flexibility** — Another benefit to employees is being able to choose the tools that they are trained on. Sometimes a latent talent just needs to be nurtured, and nothing motivates new learning like sincere interest.

As Steve Morgan, founder of Cybersecurity Ventures, notes, "Every IT position is also a cybersecurity position now… Every IT worker, every technology worker, is (or should be) involved at some level with protecting and defending apps, data, devices, infrastructure, and people."

How to Begin Your Upskilling/Reskilling Journey

Both upskilling and reskilling are poised to be instrumental in helping SOCs survive the demands of an unprecedented threat landscape, job market, and technological economy. Here's how to begin your journey with a few simple steps.

- **Conduct skills forecasting** — First, see what skills already exist within your ranks so you can see what's missing. This will let you know which areas can present the greatest opportunities to both your employees and your business. Capture the Flag (CTF) events can be a good way of vetting current cybersecurity skill sets. Once you have benchmarked your prospects, you can identify trending threats and see what skills your team is missing to get them from where they are to where they need to be.
- **Identify existing talent** — Now, look outside the ranks of your cybersecurity team. Which employees are hungry to make the shift or possess transferrable skills? In addition to those with current cybersecurity skills (the ones you just vetted in Step 1), these non-cyber workers will be wonderful candidates to reskill to fill those identified gaps. While those with a background in IT or software development may be obvious choices (and should be explored), keep in mind the intangibles like curiosity and persistence.
- **Promote a culture of reskilling** — Let your employees "choose their own adventure." Make it company-wide knowledge that those looking to advance their careers or expand to a different area of interest will be supported in their efforts to reskill and given the resources they need. This effort should be top-down. Not only should the CEO announce this new initiative, but managers should also be ready to encourage employees at the ground level and make adjustments as needed to realistically implement the upskilling and reskilling program.
- **Develop new career pathways** — "Cybersecurity is becoming less of a gatekept industry. Many of today's organizations follow a more creative approach to hiring," notes an article on Hack The Box. If someone approaches the role from a traditional route or without the usual certifications, remember what can't be bought — all the intangibles — and know that training can carry a motivated person the rest of the way.
- **Provide mentorship programs** — Mentorship programs can speed up the learning process by pairing veterans and high performers with those still new on the job. Experience is the greatest teacher, and the right mentors will be able to quickly address questions, share tribal knowledge, and help create a pool of confident, "ready-now" leaders.

Strategic Upskilling and Reskilling

Proactive Security Focus

It's good to trust. But it's better to verify.

Without the proper skills onboard, you'll never be able to fully do either. That's why upskilling and reskilling are so imperative in a proactive security space. These are skills that not every company typically has on-hand. A handful of cyber-mature organizations run their own robust offensive security programs in-house, but those without similar means may lack the ability to verify defenses at a time when security budget cuts make current defense capabilities matter the most.

At this point, you've invested in your security strategy, but have you verified its effectiveness? A great deal depends on how your unique infrastructure is set up, and how your tools and software are configured. What you think might be deployed properly, patched correctly, or integrated securely might actually not be. And you don't want an attacker to be the one who finds that out.

Enter proactive (or offensive) security: the triumvirate of vulnerability management, penetration testing, and red team engagements.

- **Vulnerability Management** — Tests for known vulnerabilities (CVEs) within your network and prioritizes them using risk context. Also comprises a patch management program to stay ahead of discovered weaknesses.
- **Penetration Testing** — Tries to exploit the discovered vulnerabilities to see if they can be compromised.
- **Red Teaming** — Assesses your defenses and incident response abilities (in both your technology solutions and SOC) by leveraging the same advanced tactics as today's cyber adversaries.

Operating on an offensive security level is just that. A threat actor can't hit you where you're weakest if your pen testers just identified that security last week and your team already repaired the damage. A cybercriminal can't sneak up on vulnerabilities you're aware of and have patched, and nation-state actors can't throw your team off its balance with advanced tactics they met last month in a red team engagement. Strong offensive security techniques clearly give your organization the upper hand.

What happens if you don't? You already know what's at stake. Besides giving an obvious tactical advantage to cybercriminals, failing to prove your defenses before you trust them (and your reputation, career, and bottom line to them) can result in disasters like:

- **Getting caught off-guard** — Because adversaries are always pushing the needle when it comes to new techniques, we must, too. That means keeping abreast of the latest in polymorphic malware, Ransomware-as-a-Service, AI-driven threats, and more. Teams that don't stay ahead fall behind.
- **Compliance fines** — Adversaries aren't the only ones looking for holes in your defenses. Auditors can spot non-compliant systems and fees and penalties follow. Some businesses aren't equipped to weather the storm: a single HIPAA violation can cost up to $50,000 per violation and the penalties for crossing SOX can exceed $5 million dollars and include 20 years in prison.
- **Firings and layoffs** — Gartner predicted that by 2024, 75% of CEOs would be held "personally liable" for data breaches. While the actual figures remain anecdotal at best, the upward trend of cybersecurity being seen as a business initiative will spread culpability beyond the SOC when a breach takes place. A recent study noted that in North America, 32% of all breaches resulted in a C-level losing their job. Additionally, and unfortunately, the fear of impending job loss is so severe that 40% of cyber teams admitted to not reporting a data breach in favor of job security, according to new research.
- **Reputational damage** — A new study indicated that as many as 75% of consumers would "sever ties" with a company following a successful data breach. Under the same circumstance, publicly traded companies lost an average of 7.5% of their stock value. And public relations costs (already sky-high following a breach) are sure to spike further if it is discovered that the error could have been easily prevented by simple best practices like offensive security techniques.

It's important to remember that proactive security doesn't just prevent breaches; it also minimizes damage by implementing safeguards so that a single entry point doesn't allow an attacker full access to critical assets. At all steps of the way, offensive security techniques discover ways to prevent attacks and mitigate fallout.

Best Practices

Our *2024 Penetration Testing Report* revealed that "83% of respondents still prioritize running at least one to two pen tests a year in order to prioritize risks, close security gaps, and stay compliant with important security regulations."

Not surprisingly, they work. Per the same report, 72% of respondents reported that "penetration testing has prevented a breach at their organization." The difficulty then seems to be means, not motivation.

The cybersecurity industry is at a stage where budgets are increasingly tight. Although the demand for qualified cybersecurity experts remains high (the cyber talent crisis still threatens to reach 85 million workers by 2030), difficult decisions are having to be made now that funding is being cut for cybersecurity programs around the globe (and at every level).

Consequently, companies are looking for ways to re-work the resources they already have. Perhaps, to find something they didn't see there before.

As they do so, it is important to run each security service through a cost/benefit analysis. We'll skip the detailed figures, but there is a definite opportunity cost to not engaging in a strong offensive security program. In our blog, "Weighing the Risk: The Cost of Skipping Pen Tests," we note that "When an organization is blind to its weak spots, it is at risk of being surprised by attackers and thrown into the limelight unprepared."

Additionally, while we can admit there is some cost to reskilling IT admins to be pentesters, "all good things come with a price. But the truth is that when stacked against the million-dollar threats of today's data breaches, an increasing number of multi-million-dollar compliance fines, and unenumerated reputational damages, the price is the lowest possible cost of staying safe."

User-Friendly Offensive Security Tools

When focusing on re-purposing your current workforce, one thing you don't want to worry about is repurposing a complex security stack, too. The right offensive tools can make all the difference in streamlining your training and getting results quickly.

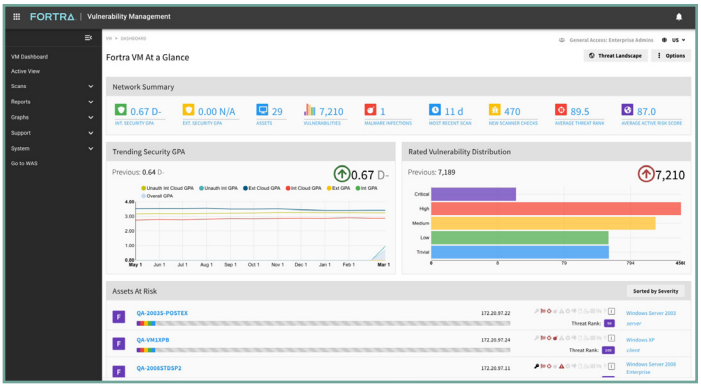
- **Fortra's Core Impact (Penetration Testing)** — Fortra's Core Impact is designed so that even junior administrators can run professional penetration tests using the same types of attacks found in the real world. With the ability to launch penetration tests across your entire infrastructure — endpoints, web applications, and client-side — you can centralize testing and maximize your investment.

  Core Impact is perfect for upskilling and reskilling employees in an offensive security space because the automated pen testing capabilities lower the learning curve for new security administrators. Now, newly cross-trained workers can give real-world penetration tests and get real-world, actionable results with even the most basic of skillsets and our enabling platform. This not only benefits your security strategy but demonstrates a quick ROI to project stakeholders.

Once employees are fully retrained, tools like Fortra® VM and Cobalt Strike can help them carry even more weight on the offensive security team.

- **Fortra Vulnerability Management** — Using Fortra VM, organizations can run automated scans with proprietary technology and gain visibility into their environment. Using the latest release, organizations can scan remotely, and immediately report malicious activity to third parties for remediation.
- **Fortra's Cobalt Strike (Red Teaming)** — Fortra's Cobalt Strike puts your people and your processes to the test with adversary simulations and red team operations that mimic the moves of advanced threat actors. This stress tests your incident response capabilities and the ability of your SOC to perform under fire, just like in a real-world attack scenario.

For a full lineup of Fortra's offensive security solutions, click here.



Fortra VM Dashboard

Conclusion

If there is poor cybersecurity, all the Ops managers and IT administrators in the world won't be enough to keep your systems online. Upskilling and reskilling your current workforce with critical offensive security skills lets employees wear multiple hats, defend your enterprise, and be where they're needed the most.

Rather than stretching your current security resources thin playing the reactive security game, offensive security measures like habitual vulnerability scans, pen tests, and red team engagements will ensure your SOC is used most wisely and can defend and respond to attacks on their own terms — not the attacker's. By upskilling and reskilling the workers who know your organization best, you can support your team with additional hands and stay agile in a shifting threat environment.

FORTRA®

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.