the GORILLA GUIDE® to...

Skills, Success, and Surviving Cybersecurity

Lifelong Learning for Organizational Achievement

KATHERINE GORHAM

SIMSPACE

POWERED BY ActualTech MEDIA

Skills, Success, and Surviving Cybersecurity

By Katherine Gorham

TABLE OF CONTENTS

ACTUALTECH MEDIA

6650 Rivers Ave Ste 105 #22489 | North Charleston, SC 29406-4829

www.actualtechmedia.com

Publisher's Acknowledgements

EDITORIAL DIRECTOR

Keith Ward

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

CREATIVE DIRECTOR

Olivia Thomson

SENIOR DIRECTOR OF CONTENT

Katie Mohr

WITH SPECIAL CONTRIBUTIONS FROM SIMSPACE

Cyndi Gutowski, Director of Cyber Security Campaigns

Pete Hay, SimSpace Lead Instructor

Gregg Ogden, Director, Product Marketing Manager

ABOUT THE AUTHOR

Katherine Gorham is a writer and editor with a focus on information security. She excels at information synthesis and can truly understand how all the pieces of complex modern information systems fit together ... and how they can be vulnerable to attack.

Introduction

Cybersecurity is a field that experiences significant professional attrition. The annual Voice of SecOps report found that up to 45% of cybersecurity professionals are considering leaving the field due to stress. Similarly, ISACA's State of Security 2022 report finds that 60% of respondents are having trouble retaining cybersecurity professionals.

Burnout in cybersecurity is a very real concern, and the remedies for this problem aren't as straightforward as simply increasing pay (although that can help). Alleviating burnout requires obtaining and retaining enough skilled cybersecurity professionals to do the job.

Cybersecurity has both a talent and a skills gap.

Unfortunately, cybersecurity is a large and diverse field, meaning that cybersecurity professionals aren't easily interchangeable. Even if the technical skills were fungible—onboarding new staff costs time. Staff turnover affects team cohesion, while new staffs need time to learn business processes and train on company-specific applications and other necessary skills.

Cybersecurity has both a talent and a skills gap. To address the talent gap, you must address the skills gap, too: In other words, you can't hire your way to a secure network—training simply must be part of the solution.

Saying "training must be part of the solution," however, is a lot easier than actually implementing a training program. "Training" covers many approaches, ranging from a very hands-off "encouragement of lifelong learning" through to systematized drills, and everything in between.

Which approaches are most helpful in meeting today's cybersecurity needs? And if training is only part of the solution to securing our networks, what else do organizations need to keep in mind?

Closing the Talent and Skills Gap

Addressing the cybersecurity talent and skills gap can be broken down into two broad categories of problems: finding talent and retaining talent. These two problems are intertwined: retaining talent is easier if you could simply add people as needed to keep stress levels manageable. Similarly, attracting talent is much easier if the existing staffs aren't all burned out, and if they can clearly see a path for career advancement.

Finding cybersecurity talent has two main approaches. The first is to hire trained cybersecurity professionals for your organization. To do this requires understanding the skills

gaps you have in your current team and using skill assessments before you make an offer. To be effective, these skills assessments should be specific to the cybersecurity industry, and regularly updated to address the rapid technological evolution that occurs in this space.

If you can identify IT professionals interested in cybersecurity, it's often worth the investment to train these individuals.

The other approach to finding talent is to identify latent cybersecurity talent and nurture it with training. Information technologists are not, as a rule, particularly difficult to find. Post-secondary institutions crank out uncountable numbers of systems administrators and developers every year, in addition to those who enter the field organically as they see their non-IT roles evolve to include IT duties. If you can identify IT professionals interested in cybersecurity, it's often worth the investment to train these individuals.

So what does training in cybersecurity look like? Traditional IT training was reasonably straightforward: vendors would release training courses for their individual technologies, and IT professionals would get certificates in those technologies. This approach works well when all you need to know is how to operate a technology.

Cybersecurity is not about how to operate a technology, but about understanding the intricacies of the interactions and dependencies between technologies, as well as between technologies and people. All the while addressing the data science challenge of sifting through millions of records, to find thousands of anomalies, and make determinations on which of those are malicious, and which are simply anomalous.

Cybersecurity requires training people both at the individual level—such as training people in the use of individual technologies—as well as at the team level. Cybersecurity professionals need to work together as a team to succeed, and the cooperation will involve bringing together expertise in multiple different technologies, and even entire domains of cybersecurity knowledge.

Cybersecurity practitioners need to be able to share knowledge and expertise, learn from one another, maintain a consequence-free environment during high-pressure events, and then be able to review and refine existing business practices afterwards.

This makes "lifelong learning" a critical consideration for cybersecurity professionals: But knowing individual technologies or domains isn't enough. Team-based training is critical to uncovering how technologies interact with one another, as well as how humans will interact with (and attempt to circumvent) those same technologies.

Understanding how humans will attempt to circumvent technologies often requires working with people who aren't technology or domain specialists. How would someone unfamiliar with a given technology attempt to use that technology to do their job? The less familiar someone is with the technology, the more likely they are to find unexpected ways to overcome perceived gaps in functionality. This is valuable information for security teams.

The necessity of working in groups, both to understand how technologies interact, as well as how people actually use those technologies, creates a need for "soft skills" among cybersecurity professionals. Cybersecurity professionals need to be leaders within their organization, and they must be trained as such.

Cybersecurity requires training people both at the individual level—such as training people in the use of individual technologies—as well as at the team level.

To find the right people, we must change how we conceptualize competence and measure expertise to tap talent that doesn't come with easy-to-categorize post-secondary diplomas. To retain those people, we need to help them keep their skills up to date, and that requires relying on multiple training modalities, including team-based exercises, as well as leadership training.

The Intersection of Workforce Readiness and Business

Today, organizations are trying to close the gap by making use of specialists in third-party consultancies. To understand where this approach is useful, and where training is a better solution, we need to better understand how cybersecurity interacts with the non-technical aspects of an organization.

Perhaps the most important concept to address is that the term "cybersecurity" is outdated. In the real world there's little—if any—real distinction between cybersecurity and any other kind of security (see **Figure 1**).

Defending the information stored on a computer also means defending physical access to that computer. It means monitoring and refining the rules around access to the information

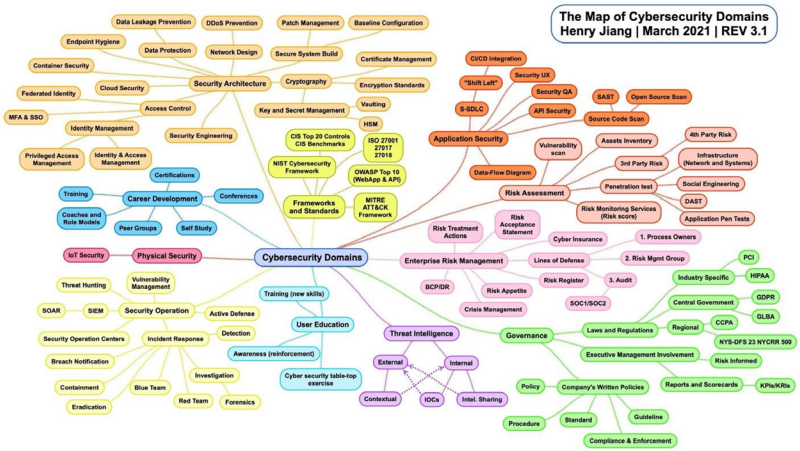


Figure 1: A map of cybersecurity domains

on that computer. Computers talking to one another over a network must be monitored, and the rules of access constantly reviewed and adjusted.

"Cybersecurity" is inseparable from "security," and security covers every aspect of the business. Physical security, business processes, Information Technology (IT), Operational Technology (OT), and Supply Chain Management (SCM) are all areas of concern for cybersecurity professionals. Cybersecurity teams need to be part of discussions relating to each of these domains within your organization.

The necessity of working in groups, both to understand how technologies interact, as well as how people actually use those technologies, creates a need for "soft skills" among cybersecurity professionals.

The integration of cybersecurity teams into wider corporate decision making has value on multiple levels. According to a SimSpace survey, 71% of IT leaders say they're not prepared for cyberattacks, while only one-third of companies surveyed say they're unprepared. These numbers indicate a significant disconnect between how IT leaders perceive their security readiness and how other leaders within the organization perceive their security readiness.

To secure your information, security needs to be a consideration anywhere information is created or used. For large or particularly siloed organizations this can seem daunting: integrating cybersecurity teams into the "business" aspects of an organization is often one of the most difficult aspects of developing a successful and sustainable approach to cybersecurity. But this approach helps to solve both practical cybersecurity problems and talent problems.

Integrating your cybersecurity professionals into other aspects of your organization helps empower them to feel they have a say in the areas of your organization that they'll be responsible for defending.

It also opens up career paths. Cybersecurity professionals who are trained in leadership and work across business units to develop and refine business processes, for example, may view a lateral career move out of their existing security role into a leadership role as an avenue for career growth.

Opening lateral career growth paths for cybersecurity professionals is good for morale—people like options—and provides another option for retaining cybersecurity talent. Business leaders with a cybersecurity background are rare, but highly valued: these individuals help organizations transform their business quickly and safely to take advantage of emerging technologies.

One example of where the integration of cybersecurity teams into the rest of the business provides outsized returns is automation. Automation is generally how organizations increase their efficiency—but automation is difficult, complex,

and requires professionals who are trained in both system functionality and the complex ways that systems interact with people, and other systems.

Cybersecurity, as a field of endeavor, is the science and art of understanding how systems and people interact. Automation is a huge part of dealing with IT and OT infrastructure. It requires reviewing and adapting business processes. And it requires modeling, testing, and adjusting approaches based upon how systems and people react at scale.

All of this makes both domain-specific knowledge and the ability to apply that knowledge beyond that domain (such as automation) key skills for security professionals. As a result, a successful cybersecurity team will be diverse in both skills and approaches to problem resolution. Your attempts to obtain and retain talent will need to be flexible as well.

You'll need to employ people who are specialists in your organization's demands and processes, but are likely generalists at security. You'll also need specialists in specific security domains, but who may only be generalists in the needs of your specific company.

In the short term, outsourcing can help to source hard-to-find, domain-specific talent. In the long term, however, training is the best approach. Outsourced cybersecurity specialists often don't have time to learn the intricacies of your organization. Given the interconnected nature of cybersecurity, a completely siloed approach to security is unsustainable.

Improving Workforce Readiness

So, if certifications and post-secondary credentials aren't the quick-and-easy solution to finding the right cybersecurity professionals, what does a successful approach to identifying and training cybersecurity talent look like?

In terms of static knowledge ("book learning"), one thing to look for is proficiency with existing cybersecurity frameworks, such as NIST or Mandiant. Certifications and frameworks, while time consuming to learn and narrow in focus, are helpful for domain specialists. They may even be required under certain regulatory regimes.

The integration of cybersecurity teams into wider corporate decision making has value on multiple levels.

Certifications and frameworks are, however, less applicable to the generalists who work more on the intersection of technologies, or of technologies and people—and this is a talent space critical to the success of any cybersecurity team. Expanding upon the rote knowledge of a certification (or the mastery of a single technology) requires a "dynamic learning" approach.

Post-secondary education, industry training in specific technologies, and generalized certification all teach different things. In addition to this, industry conferences, such as Black Hat, DEF CON, RSA, as well as community groups such as BSides, all provide valuable education opportunities.

If you're looking to hire new talent, SimSpace partners with academia. They also offer candidate evaluations, which can assist with hiring decisions, and can help identify candidate skillsets to match job descriptions and desired qualifications to real-world job functions.

If you're looking to organically grow your existing talent base, SimSpace offer a Security Organization Personnel View and Assessment, which provides organizational leadership with a view of professionals at each level within organization. SimSpace provides cybersecurity training similar to college-level courses and can help both organizations and individuals manage career progress and set goals. This reduces stress on existing cybersecurity staffs, helping to reduce turnover.

Certifications and frameworks, while time consuming to learn and narrow in focus, are helpful for domain specialists.

Perhaps most importantly, SimSpace employs a high-fidelity cyber range capable of operating at a global scale (from tens to thousands of VMs), where security professionals

can safely test their skills, both individually and as a team. Here, they can move beyond rote memorization and gain practical experience.

SimSpace training environments also employ advanced user emulation and traffic techniques, and teach both threat hunting and cyber defense. Training includes:

- Training in known Tactics, Techniques, and Procedures (TTPs)
- Intra-team exercises such as "King of the Hill" challenges
- Inter-team challenges like "Castle vs. Castle"
- Classic training against automated attacks with an extensive catalog

LIFELONG LEARNING FOR ORGANIZATIONAL SUCCESS

Succeeding at cybersecurity training, however, requires more than simply hiring a company to make the problem go away. How we think about security, and the role of cybersecurity professionals, within our organizations must change.

Cybersecurity professionals are going to be more than just those people within your organization who have "security" in their job titles. Part of this is that "security is everyone's responsibility," but a larger part is that key aspects of cybersecurity are fundamentally a part of other job roles within the organization.

Consider, for example, software developers. Ideally, developers should design security into their solutions from the beginning, avoiding the security problems in the first place. This "DevSecOps" approach, however, requires helping developers understand the different aspects of cybersecurity, and how development decisions they make will have a lasting effect on the solution they are developing, and on the organization as a whole.

But it is not enough to make a training program available, or to mandate that everyone take classes. IT personnel (especially cybersecurity professionals) are already overworked. For training to be viewed as anything other than an additional burden, that training must provide clear value to the individual, as well as to the organization.

Straightforward incentives, such as monetary rewards, may not be enough to fully engage staffs in training. In a labor-constrained market this is a weak differentiator, especially when individuals feel the pressure of various deadlines.

Ensuring that time is made available to cover training, as well as making use of different training modalities, can also be helpful here. Using a "cyber range" with multiple different challenges (such as those offered by SimSpace) allow IT professionals the opportunity to improve their skill set in a fun, challenging environment that operates at team level.

Training in "soft skills," as well as moving beyond specialization into architecture (including business architecture considerations, such as finances, business processes, and so on) can also help. This sort of training not only helps

individuals understand how technologies and people interact, but it helps people feel as though there is room to grow in their careers. All of us like feeling as though we have lots of options.

Lastly, partnering with a third-party training organization can help your people make training a priority on their own, assuming that leadership stands behind them taking the time to engage in that training. A third-party often feels more neutral than training created within one's own organization; third parties tend to focus on industry trends instead of the complexities of an organization's own internal politics or short-term goals. This helps people feel as though their training will be applicable beyond their current role, and important part of managing stress.

Learn More

In the end, the best training solutions should offer tailored learning experiences, with on-demand access to hands-on learning content. They should also provide in-depth content on specific topics and facilitate role-based skills and career development. Perhaps most importantly, there should be access to team-based training modules that deliver the experiences and hands-on challenges needed to ensure your entire security program is working as one.

Learn how a cybersecurity training range can improve your HR profile by getting in touch with SimSpace for a demo today.

About SimSpace

SimSpace delivers the most comprehensive cybersecurity risk management platform, instilling confidence in an organization's cybersecurity talent and technologies. With SimSpace, security teams, operational processes, and environments are continuously tested, readily available, and optimally tuned to defend against advanced adversaries. SimSpace: Secure with Confidence.

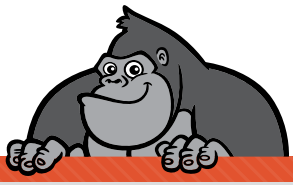
About ActualTech Media

ActualTech MEDIA

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.



If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit https://www.gorilla.guide/custom-solutions/