IMMERSIVELABS

THE ULTIMATE CYBER SKILLS STRATEGY CHEAT SHEET

INTRODUCTION

We know you're tired of reading about the cyber skills gap; many organizations are obviously facing challenges in recruiting, skilling, and retaining security professionals. We haven't written this cheat sheet to tell you what you already know. Instead, we will outline a realistic strategy for workforce-wide cyber skills development, focusing on the solution, not just the problem.

THE STATE OF CYBERSECURITY SKILLS

88%

of UK data breaches are down to human error*

Even though cyber threats are constantly evolving and attacks come from everywhere, most training for security teams is stuck in the 90s.

Classroom-based courses don't only fail to keep pace with the nature of threats; they also limit research and discovery. These courses, which comprise one-dimensional teaching and require significant time commitments – often in uninspiring environments — are impractical and expensive, moving only as fast as the slowest learner in the room. Worse still, the content is outdated within days of completion, sometimes sooner.

The evolving threat landscape demands continuous development of skills. You cannot take a snapshot in January and publish those findings in March because the content expires; however, many training providers still prepare content this way. The average data breach costs $3.86 million. By studying security fossils instead of active threats, organizations are putting themselves in financial peril.

Traditional courses don't only lack up-to-the-minute content; they disengage inquisitive minds. Cybersecurity is highly technical and cannot be mastered in the classroom, which focuses on instruction rather than facilitation. Those who excel in the field are analytical, curious and creative — the sort who break things just to understand how they work. They learn by doing and respond best to experiences that are interactive, challenging and fun.

Constraining modern learners by time and space — i.e. classroom sessions — is archaic. They can order food or watch their favourite TV show on demand, so developing cyber skills should be no different. LinkedIn's Workplace Learning Report 2019 found that 74% of employees want to learn in their spare time. One-shot training simply cannot facilitate this.

* Information Commissioner's Office (ICO)

TWO CYBERSECURITY TRAINING MYTHS

There are two main reasons businesses still risk wasting money on training that doesn't really meet the demands of their cybersecurity:

01 THERE'S A RELIANCE ON CERTIFICATIONS.

Employees who are 'qualified' in cybersecurity tick certain boxes for an organization and prove that the company has addressed the issue.
The perception is that they can be left in control with no additional training because, technically, they are qualified. The truth, however, is that most cybersecurity certifications are theory based, requiring little demonstration of real-world skills.

02 ORGANIZATIONS ARE NOT AWARE OF THE VIABLE ALTERNATIVES.

And until recently, there weren't any. But purchasing dry, static training courses that lag behind threat actors and their tools is no longer the best (or only) option. With on-demand access to the right learning experiences, employers can nurture cyber talent across an entire workforce.

CYBER SKILLS DEVELOPMENT PHILOSOPHIES

Addressing the challenge of skills in cybersecurity is not as simple as uploading training content to an intranet or even mandating classroom-based courses for individuals and teams. Your approach to enhancing cyber skills will be most effective when it aligns to your overall security strategy. This means deciding the expertise you want staff to develop (and understanding why) while considering effective methods to ensure that it sticks.

The following sections will help you understand how your security ethos can be effectively mapped to your cyber skills development efforts.

THE CAPABILITY-DRIVEN ORGANIZATION

BUILD YOUR OWN SECURITY PROS

Most organizations today are capability driven, concerned with having the right people in the right places; they rely on their staff having industry-recognized skills and qualifications, and look for individuals to fill specific functional roles (SOC Analyst, Incident Responder, Vulnerability Management, etc.). The effectiveness of their security strategy is measured against having the right people in these roles.

This approach relies on making the right training available to the right individuals at the right time. Executed effectively, a capability-driven strategy can be deployed to focus on upskilling existing talent to fill particular roles by meeting specific training objectives. The ultimate aim of this philosophy is to scale back on the significant effort and investment required to hire in individuals with these skills.

Potential drawbacks to this approach:

- Security professionals may end up siloed in roles that are too tightly defined
- Where talent isn't nurtured, hiring in may become the default

EXAMPLE FRAMEWORKS

NIST

CREST

CYBER SKILLS DEVELOPMENT PHILOSOPHIES

THE RISK-DRIVEN ORGANIZATION

MAP SKILLS DIRECTLY TO THE THREATS YOU FACE
Risk-driven organizations are typically those with a higher likelihood of being attacked, such as banks, healthcare providers, and any business with a wide digital threat surface. Employees in these organizations need the collective skills to mitigate the risks most relevant to them.

Traditionally, a risk-based approach forms the key elements of any security strategy, especially when it comes to technology and process; however, people are often excluded despite their importance in incident detection and response.

Potential drawbacks to this approach:

- Upskilling options are not specific enough to the identified risks
- Training is not flexible enough to offer relevant content on actual cyber risks

EXAMPLE FRAMEWORKS

MITRE | ATT&CK®

THE CYBER KILL CHAIN®

FRAMEWORK MAPPING

In any organization, it is critical that the security team has the skills to oppose cyber threats. But how can security leaders be certain which skills are present and which are missing?

Tangible metrics have long been absent, but this is now changing with the emergence of cybersecurity frameworks, which bring vital context and structure to the field.

> *"MOST ORGANIZATIONS STRUGGLE BECAUSE THEY DON'T KNOW WHAT CYBERSECURITY SKILLS THEY NEED, OR THEY PUT TOO MUCH WEIGHT ON CERTIFICATIONS. THEY HAVEN'T MAPPED EVERYTHING BACK TO A WORKFORCE STRATEGY OR FRAMEWORK TO FIGURE OUT WHAT THEY NEED. WE HAVE TO LOOK FOR ALTERNATIVE, EMERGENT TECHNIQUES THAT WE CAN USE TO NOT ONLY SOURCE THESE PEOPLE, BUT BUILD THEM."*
>
> *Sam Olyaei, Director,*
> *Security & Risk Management*
>
> Gartner

FRAMEWORK MAPPING

Below are examples of how frameworks designed to standardize areas of cybersecurity can easily be applied to skills development:

ALIGNING SKILLS TO SECURITY ROLES WITH THE NICE FRAMEWORK

The National Institute of Standards and Technology (NIST) has created one of the most prevalent frameworks — the National Initiative for Cybersecurity Education (NICE) Framework. According to NIST, the NICE Framework aims to 'energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development'.

Your organization can benefit from NICE when defining, developing and assessing its own cyber skills – but only if your cyber skills program of choice maps its content to the NICE framework. Many training providers use NICE to create road maps for specific job roles; for example, a provider may line up 12 exercises that, when completed, will allow the learner to apply for — and carry out — a Vulnerability Assessment Analyst role.

NIST's official documentation states that employers and security leaders can use the NICE Framework to achieve the following:

- Inventory and track their cybersecurity workforce to gain a greater understanding of the strengths and gaps in knowledge, skills, and abilities and tasks performed;
- Identify training and qualification requirements to develop critical knowledge, skills, and abilities to perform cybersecurity tasks;
- Identify the most relevant work roles and develop career paths to guide staff in gaining the requisite skills for those roles; and
- Establish a shared terminology between hiring managers and human resources (HR) staff for the recruiting, retention, and training of a highly specialized workforce.

FRAMEWORK MAPPING

ALIGNING SKILLS TO RISK WITH MITRE ATT&CK™

MITRE ATT&CK™ is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. This is used as a foundation for the creation of threat models and methodologies in the private sector, government, and in the cybersecurity product and service community.

Cyber skills content can be mapped to techniques within the MITRE ATT&CK™ Framework to help organizations visualize their cyber risk, address skill gaps and upskill in the right areas. This takes the guesswork out of upskilling for the risk-driven organization, who can ensure that employees are boosting skills that will protect the business's interests.

At present, many training programs and certifications teach skills that are not useful in the real world. Or, perhaps the skills being taught are useful — but not to the organization paying the course graduate's wages.

MITRE ATT&CK™ allows employees to take a proactive approach to learning. It enables them to visualize their business's risk profile and map those risks to specific attackers and their tactics. Perhaps a healthcare organization is at risk from a certain APT group; the security team can do their research to see what tactics said group are using, and then begin ticking off skills against the framework. This is a more focused way of learning cyber skills than taking a shot in the dark or trying to cover all bases, and it means inexperienced staff members can still be extremely useful.

THE POWER IN CONTINUOUS CYBER SKILLS DEVELOPMENT

Whatever approach an organization takes to filling skill gaps or mitigating risks, in practical terms, the ultimate objective remains the same: upskill and engage existing talent.

The key to this is handing power to the learner. Forget biannual training days — you should look to provide staff with a SaaS cyber skills solution that's available 24/7. Cyber learning needs to be frequent to be effective; attackers move rapidly and boast first-mover advantage, so those opposing them have to continually develop too.

Self-guided learning is extremely effective. Given the right tools, people can teach themselves practically anything — cybersecurity included. Professor Sugata Mitra proved this with his 'hole in the wall' experiment, as detailed in his 2013 prize-winning Ted Talk.

over 50%

of cyber experts feel their employers don't provide sufficient training*

* Information Systems Security Association (ISSA)

IDENTIFYING NEW TALENT IN UNCONVENTIONAL PLACES

1 in 5

cybersecurity professionals joined from a different sector*

Many businesses counter their lack of cyber skills by hiring new staff — but this is expensive, time-intensive and ultimately unsustainable. A lucrative solution is to unearth hidden talent from within your business, which already employs people with an aptitude for cyber.

The first step to unveiling hidden cyber talent goes against everything you know about recruitment: you should consider ditching the CV. You are not seeking experience and pre-existing hard skills, but personalities and attributes.

To identify those with cyber potential, look out for these tell-tale traits:

- Perseverance
- Curiosity
- Creativity
- Competitiveness

The best prospective cyber professionals want to learn, not be taught, which is why 63% of Immersive Labs users named 'willingness to learn' the key characteristic for cyber employees.

As well as knowing what to look for, you need to know where to look. While the obvious solution is to raid the IT department, you can also screen those in analytical and strategic departments such as finance and marketing. Those from non-technical backgrounds can, and do, transition into cyber successfully.

There are various sectors where individuals may have the right aptitude and natural talents to transition into cyber roles if properly enabled. Beyond the most obvious areas like networking, systems engineering and software development, you could find hidden gems in roles like financial planning, insurance, and risk analysis.

* Center for Cyber Safety and Education

IDENTIFYING NEW TALENT IN UNCONVENTIONAL PLACES

You should also take a look at your employees' backgrounds. Did they study mathematics at university, for instance, or serve in the military? Veterans typically have an abundance of transferable skills, including resourcefulness, perseverance, communication and planning. And while younger employees are adaptable in the traditional sense, those with vast experience — particularly IT workers — may embrace a new challenge, using their base skillset to flourish. A diverse workforce benefits from varied, atypical viewpoints too, allowing problems to be tackled in new and innovative ways.

OPENING CYBER SKILLS UP TO ALL

To uncover those in your workforce with cyber aptitude, you'll need to give them the tools to progress. It's important that a breadth of cyber skills content is available for your workforce — not just introductory material.

Over time, your staff's learning ability, dedication and practical suitability will become apparent. However, don't fall into the trap of thinking your cyber protégé from marketing will become a Red Team Analyst overnight, as this is unrealistic.

Using a SaaS solution with management functions, you can track your team's progression and see who is performing well and in which topics. This will help you identify staff who excel in particular areas, including any you may have highlighted as requiring skills relevant to particular risks.

IDENTIFYING NEW TALENT IN UNCONVENTIONAL PLACES

87%

of global organizations see untrained staff as the greatest cyber risk to their business*

CONTINUOUS MEASUREMENT AND VISIBILITY

New threats emerge every day, so skills development must be continuous to keep pace with attackers. Your team should have access to up-to-the-minute content that is built around the latest vulnerabilities and exploits — and delivered fast.

Utilizing training content from multiple providers is good for variety but creates challenges in measuring effectiveness and quality. It is also expensive. You should choose one provider that has a wide range of useful content and that applies threat intelligence to produce interactive exercises; this will ensure your team develops relevant skills that reduce organizational risk in real time.

It is also vital that you have visibility into your organization's security strengths and weaknesses when it comes to skills, or it can be easy to misplace your efforts. With the right visibility — something that comes from an online solution's management features and insights — you can guide your employees' development, ensuring it works for your business.

*ESI ThoughtLab & Willis Towers Watson

ELEMENTS OF A SUCCESSFUL CYBER SKILLS PROGRAM

INTERACTION AND GAMIFICATION

Traditional training content isn't engaging or relevant enough to inspire individuals who want to gather practical skills — especially when delivered in a stale classroom environment. Interactive and gamified solutions are far more effective, as they enable employees to develop skills on their own terms without disruption to company operations. This enables greater training frequency and, in turn, greater progression.

Gamification is the act of taking something already in existence — a website or application, for instance – and boosting engagement using game mechanics such as jeopardy, reward and competition. These mechanics are incredibly addictive and help get students hooked on learning. A gamified cyber skills solution might include a points system and leaderboard to promote healthy competition between individuals.

Typical gamified cybersecurity exercises such as capture-the-flags and hackathons double up as great team-building activities owing to their social nature. McAfee found 96% of organizations that hold such events report tangible benefits. They can also help in the search for hidden organizational talent, with self-taught or uncertified participants using them to prove their worth.

85%

of employees would spend more time on software that was gamified*

* TalentLMS

ELEMENTS OF A SUCCESSFUL CYBER SKILLS PROGRAM

RISK-RELEVANT OBJECTIVES

For risk-driven organizations, it is essential that employees learn skills that will actually drive down cyber risk. If your organization already has two network denial of service experts, training a third is wasteful when that individual could be learning skills to patch an organizational weakness.

A successful cyber skills program enables managers to set learning objectives for their teams. Better still, the program should have predetermined skill paths that can be assigned to learners in order to take them from novice to ninja in various areas of cybersecurity.

77%

of senior security managers said their organization would be safer if it used gamification more*

* McAfee

NEXT STEPS

The skill levels of the cyber professionals in your organization directly correlate to the strength of your security posture, as well as your capability to effectively mitigate risk. Here are some initial actions you can take to ensure the effectiveness of your own skills development strategy.

01 ENSURE RAPID SKILLS DEVELOPMENT IS INTEGRATED WITH YOUR SECURITY PROGRAM

It's well known that effective strategies rely on people, process and technology. Unfortunately, it is easy to neglect your people, who must have — or quickly be able to acquire – the skills to execute that strategy.

02 STRESS TEST THE VALUE OF CERTIFICATIONS

On the surface, individuals with particular certifications would seem to represent your most highly skilled team members, but you should examine course content to ensure it aligns with the security objectives of your organization. If you don't, there's a risk you are putting significant resources into purely academic exercises.

03 HARNESS THE POWER OF COMPETITION

Cloud-based platforms that allow for interactive and on-demand skills development also open the opportunity for individuals to compete with each other through challenges and real-world simulations. These types of activities will also help to reveal talented individuals not yet working in cybersecurity roles.

ABOUT IMMERSIVE LABS

Immersive Labs is the world's first fully interactive, gamified and on-demand cyber skills platform. Our technology delivers challenge-based assessments and upskilling exercises which are developed by cyber experts with access to the latest threat intelligence. Our unique approach engages users of every level, so all employees can be equipped with critical skills and practical experience in real time.

IMMERSIVELABS

www.immersivelabs.com | enquiries@immersivelabs.com