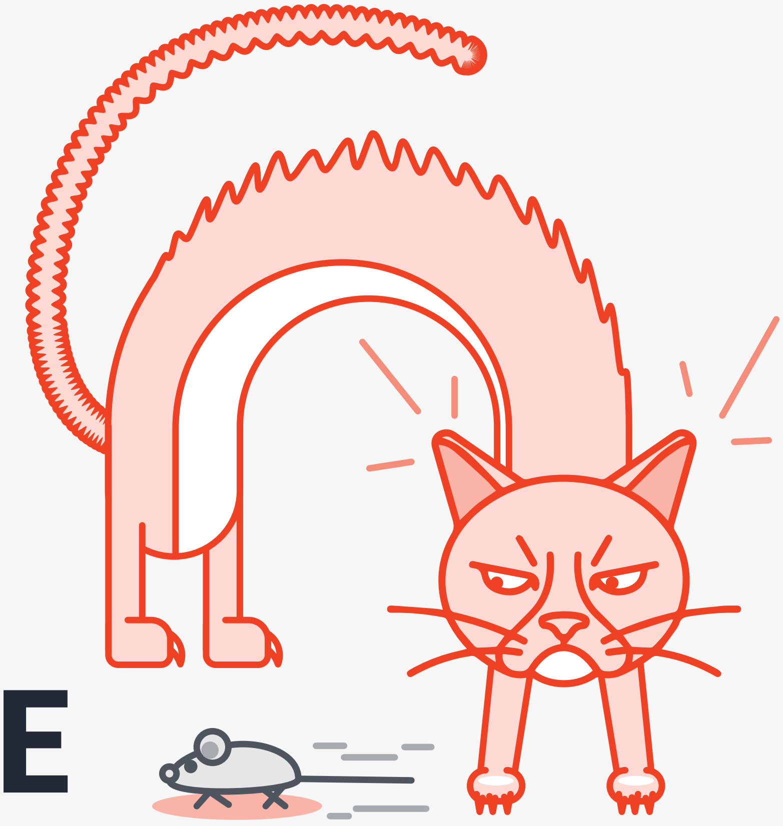
CAT & MOUSE



RESOLVING THE TRAINING CHALLENGE
FOR CYBERSECURITY STAFF

cloudshare

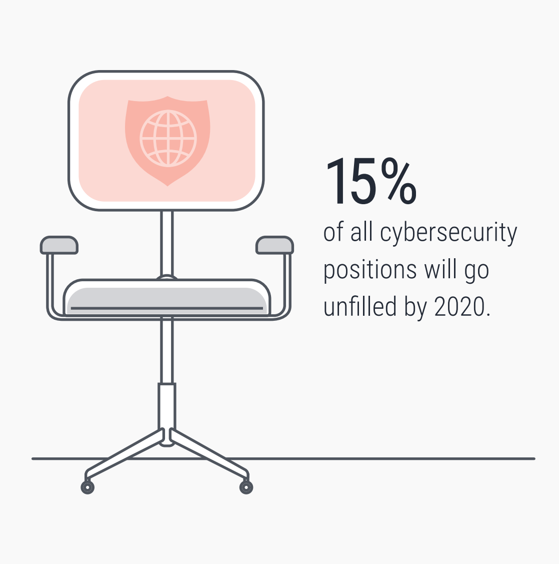
Contents

Foreword: a worrying shortage

There is a crisis in cybersecurity. A 2016 survey by Intel Security[1] and CSIS found that 82% of companies confirm they are experiencing a shortfall in their cybersecurity workforce. Worryingly, if these current trends continue, the report predicts that by the year 2020, 15% of all cybersecurity positions will go unfilled.

To compound this crisis, there are ever more[2] diverse forms of cyberattack, and companies are facing more sophisticated and sustained attacks than in the past. Nonetheless, research suggests that very few cybersecurity staff are getting the training they need to stay up-to-date. While, on a high level, more needs to be done to entice fresh talent into the industry, it is also clear that training needs to play a key role in helping to compensate for the skilled workforce shortage.

82%
of companies confirm they are experiencing a shortfall in their cybersecurity workforce.



15%
of all cybersecurity positions will go unfilled by 2020.

This whitepaper explores this issue in more detail and proposes a solution for how IT decision-makers can support and improve the training and education of their cybersecurity professionals.

Winning the cat and mouse game

Cybersecurity can sometimes feel like a game of cat and mouse. Every time experts believe they have resolved a threat, another one emerges. This turns the job into one of constantly analyzing possible threats, reverse-engineering systems and discovering weaknesses to be resolved. Cybersecurity professionals – whether they're consultants, government employees, software architects at large firms or even developers at cybersecurity companies – need to stay constantly abreast of the latest technical advancements and consistently devise creative solutions for neutralizing these threats.

While the scope of the cybersecurity challenge continues to grow, the industry is facing a dearth of skilled practitioners – a shortage predicted only to worsen. In an ideal world, there would be an abundance of skilled and well-prepared cybersecurity experts ready and able to take on any challenge. In reality, however, demand outstrips supply.

So, what can IT decision-makers do to compensate for this imbalance?

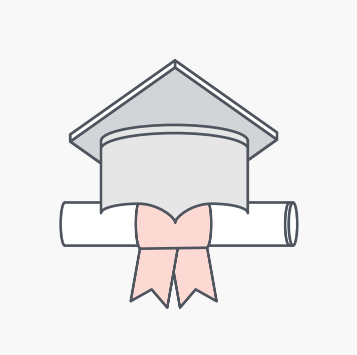
Solution	Strengths	Weaknesses
Invest more in cybersecurity software	Possession of the latest, cutting edge technology	Technology is only as good as the people who use and deploy it. Even the most advanced technology is useless without skilled implementation
Hire more staff	More people to work on projects, discover problems and maintain security. Brings in expertise from outside the company	Extremely expensive and only effective as long as the additional professionals stay up-to-date with the latest cybersecurity challenges
Regular training	Keeps employees up-to-date with the latest technology, threats, and best practices for dealing with them	Time-consuming and requires effort to manage

As this table demonstrates, simply having 'more hands on deck' does not necessarily equal the best cybersecurity defense. By contrast, having a lean team of well-trained and tested staff can make your organization better-prepared to spot attacks and deal with them efficiently.

So, how do cybersecurity professionals currently receive their training?

Current training methods for cybersecurity professionals: are they effective?

The classic route: education



A report from McAfee[3] – a leading antivirus firm – explains that for most cybersecurity professionals, traditional academic institutions remain the primary source of initial training and education in the field. Typically, cybersecurity staff are drawn from graduates with a background in computer science, who then specialize in cybersecurity – perhaps through modules and specialization during their degrees. For entry-level positions, cybersecurity professionals are generally expected to hold, at a minimum, a bachelor's degree.

While higher education is clearly the most common route into a cybersecurity career, McAfee's research also suggests that this approach is far from sufficient. When cybersecurity professionals were asked how well they thought their higher education supported them in their 'real world' jobs, only 23% felt that their education 'fully' prepared them, and 33% felt they ended their degrees only 'somewhat' or 'not' prepared for the real world of cybersecurity.

Hacking competitions

Governments and major employers often utilize hacking competitions as a means to discover fresh cybersecurity talent. Competitors take part in simulated hacking games, either acting as hackers or as cybersecurity 'defenders', attempting to resolve problems or find weaknesses within systems.

Hacking competitions are viewed as a positive way of learning new skills. McAfee's survey found that in 29% of companies, they play a particularly important role in developing skills.

Innovative skill selection: gaming

The use of games is an increasingly popular method for identifying individuals with the skills for a successful cybersecurity career. However, games tend to be used more commonly as a way of identifying those with potential than as a form of ongoing professional training.

Personal reading

There is, of course, a responsibility on the part of cybersecurity professionals to keep their own skill sets up-to-date. Conscientious employees should be expected to stay current with the latest developments and news as a natural part of their day-to-day jobs – following important cybersecurity industry websites, social media feeds and blogs.

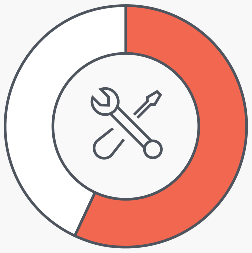
Employer-provided training

Research indicates that most cybersecurity employees receive at least some form of annual cybersecurity training. Typically, this takes the form of eLearning, which is principally theoretical. More advanced companies might offer some hands-on, practical training, yet if these courses take place only once per year or are too general in focus, their value is questionable.

Current training for cybersecurity professionals is insufficient

In sum, the current state of affairs appears dire: the constant and ever-changing evolution of new and more sophisticated threats, combined with a cybersecurity workforce reporting that their university education has left them insufficiently prepared to address them. The crucial need for more comprehensive and frequent professional training seems clear.

Unfortunately, this training does not seem to be happening. QA[4], an IT training provider, recently surveyed 300 cybersecurity and C-Suite professionals about their learning activities, while IT-standards agency AXELOS[5] interviewed professionals to find out about the kinds of training they receive. Headline findings include:



57%

of professionals they did not feel they had the right balance of skills to protect themselves.

Only 22%

of organizations plan to upgrade the cybersecurity skills of their IT teams.

82%

of organizations use traditional, computer-based IT training. **Only less than a third** offer immersive, 'real life' style training.

Fewer than half

of organizations provide ongoing cybersecurity training.

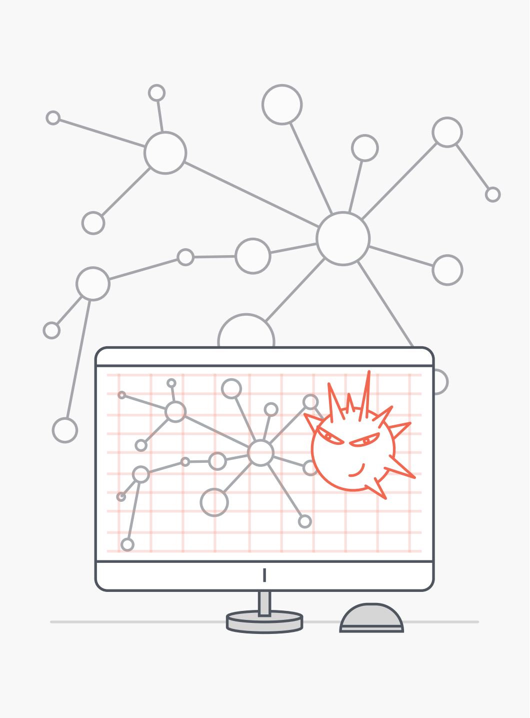
To really keep on a par with the latest threats, cybersecurity staff must have their skill sets constantly refreshed, and far more regularly than what is currently offered.

A new approach is clearly needed. In the next section of this whitepaper, we suggest a solution that IT decision-makers can employ to resolve this issue.

The next steps in cybersecurity learning

A cloud-based, lab-centered training solution offers a highly capable, flexible, risk-free and cost-effective method of keeping cybersecurity staff trained. Rather than providing abstract, generic and theoretical training, cloud-based lab training allows you to test your cybersecurity staff's reactions in scenarios that simulate real world breaches. Instead of depending on their memories of a university training course or their one-time participation in a hacking competition, you can keep your cybersecurity employees' skills sharp and relevant by offering hands-on, lab-based training.

How cloud-based lab training would work



Cloud-based labs provide a unique method of training cybersecurity staff. By using virtual machines and networks, businesses are able to rapidly build almost any type of required IT environment, then use it to deploy a realistic simulation.

For example, if a healthcare company decided to test its cybersecurity staff on its ability to respond to an attack, cloud-based IT labs would enable the creation of an exact replica of the company's network environment and the launch of a simulated attack. Since the 'attack' is carried out in a simulated, cloud-based environment that is completely isolated from the company's actual production environment (and can be built and destroyed in minutes), there is no possible chance of accidental harm to the company.

This approach is relevant in a wide range of training scenarios and could be used to replicate the latest emerging threats and to test staff to ensure they are prepared for 'real life' attacks:

Discover malware in an environment

Cybersecurity staff are told that the company believes malware has invaded a company machine. Staff are challenged to find, then neutralize, the threat.

Attack your own firewall

Cybersecurity staff is placed in the shoes of an attacker and are asked to discover and exploit weaknesses in a simulation of your own company's firewall.

Role play scenarios

Staff are asked to imagine that some rogue organization – a hacktivist group for example – has breached the company's systems and is wreaking havoc on its servers. They must find ways to end the attack and freeze the 'enemy' out. (This approach often involves pitting employees in competition against one another.)

More traditional eLearning

eLearning from specialist providers provides an enormous amount of valuable theory and insight into the latest industry expertise. eLearning in combination with cloud-based lab work allows instructors to review how trainees are progressing through various tests and exercises during the course.

These types of training are highly valuable for cybersecurity staff – challenging them to put their skills and minds to the test, inspiring them to work co-operatively with colleagues, and encouraging them to become more creative in order to find novel methods for resolving complex problems.

Because the cloud makes it easy to spin up real-world lab environments, it allows more frequent and effective opportunities for organizations to test their cybersecurity professionals' skills and push them to constantly test their reflexes.

Take back control with cybersecurity training

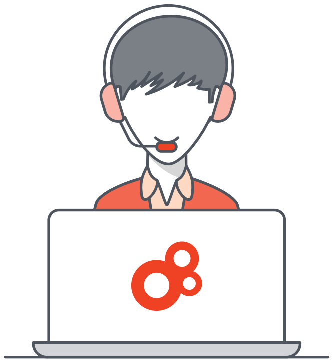
In this whitepaper, we have seen how IT decision-makers are facing a shortage of skilled cybersecurity staff. Further exacerbating this problem is the reality that far too many cybersecurity professionals receive only limited ongoing training that often provides little more than a refresher on basic concepts. To stay truly up-to-date with the pace of change in cybersecurity, companies must provide more consistent, 'real world' training.

We have seen how cloud-based training labs offer the ideal space for providing this type of instruction and how regularly testing staff with simulated games and practical exercises (along with more standard theoretical training) can keep their skills refreshed and up-to-date. Cloud-based labs offer a 'walled-garden'; they can be destroyed as soon as you have finished with them and pose no possibility of damaging your production environment.

In a world of increased cybersecurity dangers and workforce shortages, cloud-based training provides a means of updating your staff's skills in a highly practical, flexible and cost-effective manner – giving you a fighting chance in the worst-case scenario of an actual breach, and arming your staff to react quickly and confidently to resolve any situation before it gets out of hand.

About CloudShare

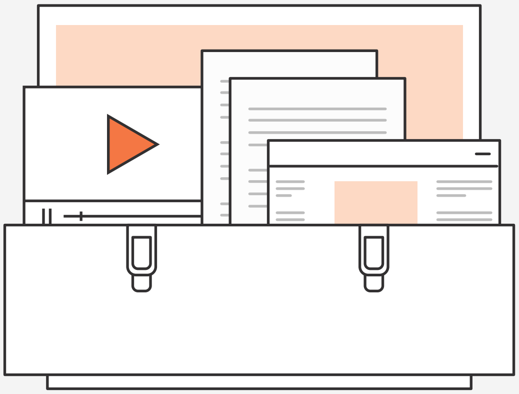
CloudShare is a leading provider of cloud-based training environments, with particular expertise in cybersecurity training. Trusted by leading organizations worldwide, our premium training lab solution is especially well-suited to support the needs of instructors and students in the cybersecurity industry.



To learn more about how CloudShare's advanced lab solutions can help bring your cybersecurity training into the real world, visit us at:

www.cloudshare.com

RESOURCES



[1] Intel. 2016. Global Study Reveals Businesses and Countries Vulnerable Due to Shortage of Cybersecurity Talent. Available online: https://newsroom.intel.com/news-releases/global-study-reveals-businesses-countries-vulnerable-due-shortage-cybersecurity-talent/

[2] Hackmageddon. 2016. 2015 Cyber Attacks Statistics. Available online: http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/

[3] McAfee. 2016. Hacking the Skills Shortage. Available online: http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

[4] Gregory, Mark. 2016. QA Uncovers the Status of Cybersecurity in the UK. http://www.thecsuite.co.uk

[5] AXELOS. 2016. UK Organizations' Cybersecurity Awareness Learning Needs to Enter the 21st Century. Available online: https://www.axelos.com/news/uk-organization-cyber-awareness-needs-to-enter-21c