(ISC)²

The Ultimate IT Manager's Guide to Cloud Security Team Development

Lack of cloud computing expertise creates security challenges

Ever since 2020, there has been a roller coaster of change for all professional environments. Businesses have become increasingly digitized and employees abandoned their offices seeking more flexible ways of working. Cloud platforms have become the new computing infrastructure. Today, 39% of organizations report that they have more than half of their workloads in the cloud, while 58% plan to make this shift in the next 12-18 months[1].

The migration to the cloud is not single faceted. Organizations quickly realized that to reap the full potential of the cloud they must leverage multiple platforms, each offering a distinct added value. In fact, more than three-quarters (76%) of organizations are utilizing two or more cloud providers, while most organizations (72%) have a hybrid or multi-cloud deployment strategy[2].

Prior to the emergence of cloud technologies, almost all technology, software, database, server and other IT requirements were managed on-premises by IT administrators with background in servers, networking, storage and more. Cloud technology has allowed businesses to shift the management of some, or all, of these responsibilities to the cloud service providers.

Cloud technology has created a growing demand for new professions, including DevOps engineer, cloud engineer, cloud architect, software engineer, security engineer and solutions architect. These jobs offer high-skill opportunities that require a variety of IT experience and skills. The job description of a typical cloud engineer demands a broad array of knowledge that crosses several IT disciplines, including computers, servers, networking, cybersecurity, data analytics, programming and cloud technologies such as AWS, Azure and Google Cloud.

With employers requiring such a diverse skill set, it is often difficult for them to fill open cloud positions. Additionally, since many cloud technologies are relatively new, it is often difficult to find professionals with lengthy experience to fill high-level and management positions. Cloud skills shortage is a concern reflected in almost all surveys[3].

- 93% of organizations are moderately to extremely concerned about the massive skills shortage of qualified cybersecurity professionals
- 52% say the main barrier to migrating to cloud-based security solutions is lack of staff expertise and 57% admit this lack of staff expertise makes cloud compliance challenging
- Lack of staff expertise prevents 40% from adopting cloud solutions for their organizations
- 56% feel that cloud security skills are the most important expertise their organizations need

The role of the IT Manager in building cloud skills

To address the cloud computing challenges and the changing security needs, training and certifying IT staff is the preferred tactic by 64% of organizations. What is more, 83% of organizations report that their teams would benefit from cloud security training and/or certification to effectively and efficiently operate and configure their cloud environments[4].

Within an organization, training is usually the responsibility of the HR department. However, cloud security is a very specialized, dynamic discipline, requiring a focused, expert-led approach. While HR oversees training as a function, the IT manager must be engaged and remain involved in cloud security training by assuming the responsibility of creating a curriculum that maps to the organization's needs and goals.

Developing a cloud security education curriculum requires proper planning, starting with a thorough assessment of the organization's needs.

1. Assessment

In assessing training needs, the IT manager must focus on the organization's needs – both immediate and long-term. Identify your organization's most pressing needs and plan the training curriculum accordingly. Since cloud security is such a broad topic, it is easy to lose sight of what is mission-critical to the organization and to employee development. Therefore, having a formal plan is essential.

2. External training and certifications

Training that originates outside the organization typically is built around certification and certificate programs, and the development of specialized security skills. Vendor-specific certificates/certifications, like the ones offered by Amazon, Microsoft, or Google, demonstrate technical expertise in the vendor's cloud platform.

A comprehensive curriculum also should include vendor-neutral certifications on cloud security, like (ISC)² Certified Cloud Security Professional (CCSP), which are built around security standards and frameworks. Vendor-neutral certifications prove the ability to implement, monitor and administer any cloud environment using security policies and procedures regardless of the vendor. Moreover, vendor-neutral certifications like CCSP are extremely valuable as they enable you to identify the cloud security leaders who understand strategy and who can design, develop and manage the overall cloud security posture of your organization.

3. In-house training

A comprehensive cloud security curriculum should include internal training components as well. While third-party programs and certifications offer valuable knowledge, cloud security professionals can learn a lot by delving into the experience of their colleagues and senior team members who are familiar with the organization's specific environments and practices.

From 'workable' to 'ideal' cloud security profiles

Despite the headlines we've seen over the past two years indicating a dire need for better protection against cyber-attacks, there is still a cybersecurity workforce gap of more than 2.72 million positions[5]. While that number has been steadily decreasing year over year, it is simply not enough. According to the 2021 (ISC)² Cybersecurity Workforce Study[6], the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets.

Building a strong cybersecurity team is a big challenge for any organization. Talent is scarce. But many organizations continue to repeat the mistakes of focusing their time and energy on hunting down and competing for a select few cybersecurity "All Stars" instead of strategically developing their teams at all skill levels to create a sustainable, long-term investment in their security personnel.

It's an often-discussed frustration among cloud security and cybersecurity professionals: too many organizations are looking for 'ideal' profiles for the positions they are trying to fill[7]. These individuals are few and far between.

Instead, IT managers need to invest on building well-staffed cloud security teams using 'workable' profiles – profiles with potential, attitude and aptitude. IT managers need to focus on new talent to sustain long-term, self-replenishing teams that will grow more experienced and confident, with junior members ready to advance and take on new challenges for years to come.

1. Pick 'workable' profiles

While technical skills and expertise are desirable, they are not imperative for every role in cloud security. IT managers should consider selecting candidates with aptitude and useful non-technical skills such as communication, creativity and problem-solving. Organizations should also recruit and train current employees who are keen to make the transition to cybersecurity. Human capital management is an essential tactic for addressing cloud security needs.

2. Look for talents

As organizations continue their journeys to the cloud, they are becoming more vulnerable to cyber-attacks and struggling to keep pace with the evolving threat landscape. Security teams need to upgrade their skills to out-think cybercriminals who are becoming more sophisticated with time and advancing technology. IT managers could look for talent at hackathons and similar competitions that bring the brightest minds together under one roof.

3. Invest in skill diversity

The multidisciplinary nature of cloud security, which includes technology, finance, risk, legal, compliance, project management, training and communications, should be embraced for its appeal to those with diverse skills, backgrounds and experiences. Tapping into new sources of talent and welcoming non-traditional pathways to cybersecurity careers can lead to a more diverse talent pool, which can be further nurtured through on-the-job training, professional development and certifications.

4. Develop talent into an 'ideal' profile
   Attackers are always evolving their skills and looking for new vulnerabilities to exploit. As talented security practitioners become more experienced, organizations need to update their cloud security skills to align with current threats. Organizations and IT managers also need to invest in continuous learning so that security team members have the appropriate skills to combat new threats. Once enough experience is gained, encouraging and supporting your staff to acquire a cloud security certification like (ISC)² CCSP is the ideal way of bringing their skills up to standard.

Technical skills building

One of the greatest challenges cloud security professionals face is the hectic pace of technology evolution. It is one of the main reasons continuous learning and skills development is so critical to keeping cloud computing environments up to date.

Ensuring that systems are kept current while underlying technology and platforms are evolving, makes it necessary to keep up with the cloud platform vendors. These vendors are good about communicating changes, updates and plans for new technologies. To keep up with technology changes, the IT manager should plan for skills updates accordingly and maintain close ties with the vendors' representatives.

Besides uplifting your vendor-specific technical skills, the IT manager should invest in developing more holistic knowledge and understanding around cloud security practices and frameworks. This is the added value of vendor-neutral cloud security certifications, like (ISC)² CCSP. These certifications are designed to ensure cloud security team members stay current with evolutions in cloud technology by learning practices, procedures and programs that focus on the wider technology and not on specific vendor platforms.

By pursuing CCSP certification, cybersecurity experts within organizations can gain a holistic understanding of cloud architecture, infrastructure, deployment models, emerging technologies and risk management. CCSP certification can benefit the security team and the organization as a whole in many ways[8].

1. Common vocabulary
   The CCSP training course covers cloud deployment models, cloud service models and much more. It helps students put all the pieces together with examples that enable them to formulate a use case and select the right deployment option.

2. Align security with business goals
   The CCSP uses the IT Infrastructure Library (ITIL) framework to enable security teams to speak in terms of business services rather than technology. Security can speak the language of business people and easily align security objectives with business needs.

3. Gain deeper understanding by studying real life problems
   CCSP candidates examine throughout the courses real life use cases and discuss how to apply the correct tools to address these issues. Using that process, students gain deeper meaning of cloud security.

4. Understand new paradigms and emerging technologies
   When moving to the cloud, cybersecurity experts need to change the way they think about protection. Traditional approaches of protection, such as perimeter security, do not work in the cloud, because corporate perimeter is obsolete.

5. Regulatory compliance
   All organizations operate within specific security and privacy frameworks. Cloud security professionals learn how to maintain compliance with the laws and regulations that are applicable for their industry in the cloud.

As organizations seek to gain the many advantages of the cloud, they need to understand the big picture of how the cloud works, its risks, as well as how to maintain a strong security posture and comply with regulations. Taking an Official (ISC)² CCSP Training Course and earning CCSP certification delivers a practical, hands-on understanding of how to maximize the cloud's benefits while minimizing risks.

Training delivery options

Different individuals learn in different ways; some prefer self-paced study with a strong emphasis on online courses and materials, while others thrive with instructor-led training, whether its online or in a classroom setting. Whenever possible, try to match delivery methods that best suit individual learning styles and the material to be learned.

Choosing the right training methods to deliver new ideas and develop new skills is important if you want to ensure proper adoption and absorption. You will often deliver the same information to a group of individuals, which can lead to choosing between delivering training in a group or individual format.

Understanding the pros and cons of team and individual training will give you a good basis to make that decision so you can choose the best training for each situation.

Team training

Team or group training is one of the most common ways to push information to a large number of people, because most can conveniently learn together under a single trainer. As noted by Peter Senge, Professor at the MIT Sloan School of Management,

> "Team learning is vital because teams, not individuals, are the fundamental learning unit in modern organizations.[9]"

While having live in-person learning is great for team training, a delivery method that is rising in popularity is private online instructor-led training, which is virtual group training. Team training provides all the advantages of upskilling your security team members which are amplified by team dynamics. The following benefits of team training are worth considering when selecting a training option[10].

- Build a team spirit
  When students learn within a team, they interact during classes, as opposed to each student watching a lecture and completing coursework alone. This type of education allows students to motivate each other, increasing retention and course completion rates. The collaborative aspects of team learning help students develop social capital and social networks, which can improve their understanding during class. It also impacts their future professional development by establishing strong social ties with their peers.

- Increase engagement
  Team members can apply their knowledge directly to the work environment, becoming more engaged in the learning process. Engaged employees are enthusiastic participants willing to invest their energy in the company's success. Not only do engaged security professionals give their best to secure their workplace, but they are also less likely to leave the company, improving retention rates.

- Boost confidence and satisfaction
  Although engagement and job satisfaction are not synonymous, engaged employees are usually much happier in their jobs. They find meaning and purpose in what they do and feel fulfilled by investing in their work. When team members can do their jobs more effectively, they also become more confident. This leads to greater job satisfaction and improved employee retention.

- Improve collaboration
  Even if your team training focuses on a technical subject area, like cloud security, your team members will practice applying non-technical skills such as critical thinking, teamwork, communication, problem-solving and flexibility. Having employees go through the experience together, discuss topics with each other and learn cognitive frameworks for evaluating and applying techniques and practices to secure cloud environments will expand their ability to work well together.

- Enhance productivity
  According to Deloitte, teams learn and adapt more quickly than individuals[11]. When all team members learn in an environment together, they can apply the skills they gain to the group's tasks. Collectively learning new ideas and methods gives team members common language and understanding to help them become more successful in meeting not only cloud security goals, but also futureproof their organization.

- Build a positive culture
  A healthy company culture embraces change, inquiry, learning and discussion and invests in its workforce through learning and development. Offering professional development opportunities to teams improves engagement, job satisfaction and overall happiness, contributing to a positive workplace culture. A learning format where team members interact helps inject a learning culture into everyday processes. Group learning encourages flexible thinking, which can set a course for your company that's both culturally and technologically resilient.

Individual training

Individual training is typically the process of using a mentor or coach to teach a specific skill or behavior to an individual, to coach them, or to work on development on a one-on-one basis. The individual can select one of the following official training options[12] to meet their needs:

- Online instructor-led, where they can choose between a 5 consecutive day online class or have the flexibility of training over an 8-week period online. This is a great option for those who want instructor-led training, but also need the flexibility of doing it online since training recorded sessions are available to view.

- Classroom-based training for face-to-face learning.

- Online self-paced, where the student has access to on-demand recorded video content. This option is great for learners who are very disciplined and need total flexibility for their schedule. They feel comfortable and stay the most focused in their own space on their own pace.

Individual training may present several advantages. For example, the students can easily receive personalized attention, or the individual's specific barriers and obstacles can be approached and tackled by the trainer. In addition, individual training may reduce downtime of the team.

Besides the benefits, there are some disadvantages to consider as well.

- Individual training does not facilitate the same retention of skills as team learning
- Individuals who learn alone may not work as well in teams as individuals who learn in teams

Conclusion

With the increasing emphasis on remote work, cloud security has become the #1 skill and the most desired area in continuous professional development. Recent surveys indicate that training and certifying IT staff on cloud security is the primary tactic organizations deploy to assure their evolving security needs are met. Interestingly, 80% of professionals admit that they and their teams need cloud security training or certification to be better equipped to operate in cloud environments[13]. This rate will continue to grow rapidly as organizations turn to vendor neutral cloud-based security solutions versus on-premise legacy ones.

Rather than chasing and competing for a limited number of highly experienced professionals, businesses should empower their employees with building strong, vendor-neutral cloud skills. Modern businesses are faced with so many challenges while moving to the cloud that investing in cloud security training is a critical business decision. As we have discussed, there are so many benefits coming from cloud team development and empowerment that investing in cloud security awareness training is investing in the future of your company.

CCSP gives organizations a competitive advantage

CCSP is an essential partner for your organization to excel in cloud security. Earning the globally recognized CCSP cloud security certification is a proven way to better secure critical assets in the cloud. The CCSP shows that your employees have the technical skills and knowledge to manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by the cybersecurity experts at (ISC)^2, the creators of the well-respected CISSP certification.

CCSP®
Certified Cloud
Security Professional
An (ISC)^2 Certification

The CCSP is the start of your organization's journey to cloud computing. Once certified as a CCSP they are required to maintain their certification through Continuing Professional Education (CPE) to ensure that their continuous professional development evolves along with cloud technology. The structured knowledge earned by holding the CCSP certification can benefit your business in multiple ways and is a sure investment into securing your organization's future success in a shifting global environment.

Your organization can benefit from both available learning options – individual or in-house team training. (ISC)^2 offers tailored training solutions centered around your organization's cybersecurity certification needs and requirements. Whether you have a global workforce that requires varied training options or a smaller staff that needs a private training seminar at one central location, (ISC)^2 delivers a solution that fits your budget, schedule and certification objectives.

(ISC)^2 is the leader in cybersecurity certifications and is acknowledged by companies worldwide. To learn how your business can benefit, check out our Official (ISC)^2 Enterprise Training Solutions. We are ready to work with you, one-on-one, to develop a targeted cloud security training and certification plan for your team. Contact our team.

To get a deeper understanding of the CCSP certification, download the CCSP Ultimate Guide.

About (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our association of candidates, associates and members, more than 235,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™.

For more information about (ISC)² visit our website, follow us on Twitter or connect with us on Facebook and LinkedIn.

(ISC)² | CC℠ SSCP® CISSP® CCSP® CGRC™ CSSLP® HCISPP®

References

[1] https://cloud.connect.isc2.org/cloud-security-report

[2] https://cloud.connect.isc2.org/cloud-security-report

[3] https://cloud.connect.isc2.org/cloud-security-report

[4] https://cloud.connect.isc2.org/cloud-security-report

[5] https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap/

[6] https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[7] https://www.wsj.com/articles/companies-urged-to-adjust-hiring-requirements-for-cyber-jobs-11606732200

[8] https://www.isc2.org/articles/how-can-ccsp-help-your-organization#

[9] https://leeds-faculty.colorado.edu/larsenk/learnorg/senge.html

[10] https://emeritus.org/blog/benefits-of-team-training-in-the-workplace/

[11] https://www2.deloitte.com/us/en/insights/focus/technology-and-the-future-of-work/high-performance-team-building.html

[12] https://www.isc2.org/Training/Enterprise-Solutions

[13] https://securityscorecard.com/resources/impact-of-covid-19-on-enterprise-it-security-teams