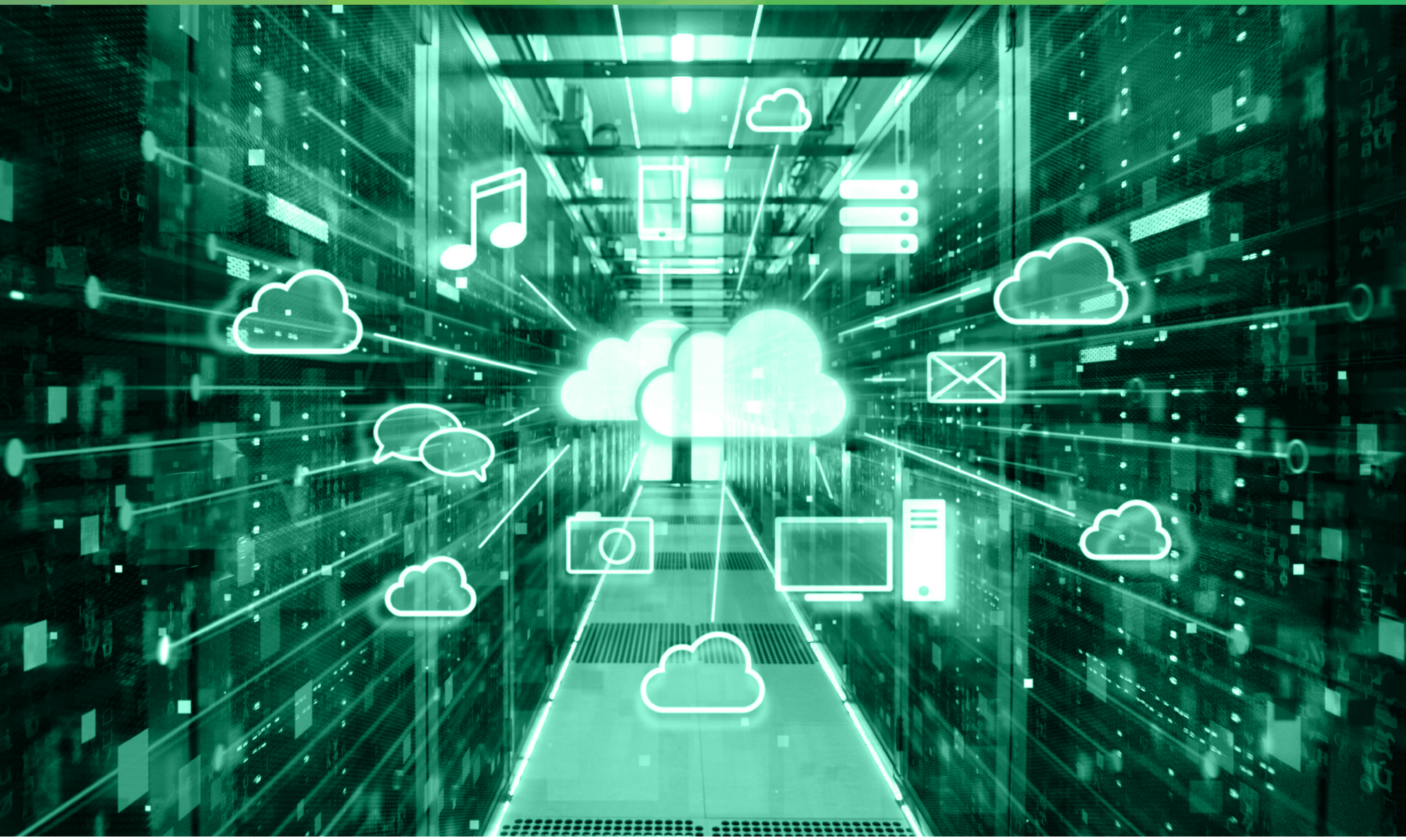

CLOUD SECURITY RISKS & HOW TO MITIGATE THEM

Transitioning to the Cloud Safely and Strategically

(ISC)² ®   CYBER THEORY

EXECUTIVE SUMMARY

Even though the cloud is promoted as more secure than ever today, companies are experiencing an increasing number of data breaches.

Why the apparent contradiction?

Often, cloud customers lack a comprehensive understanding of cloud architectures and who is responsible for securing their data. Before organizations embark on their cloud adoption journey, they must therefore gain a strategic understanding of cloud benefits, cloud architectures/infrastructure/services, and risks as well as best practices and technologies for safeguarding data in the cloud.

This white paper looks at cloud security challenges from the perspective of both Cloud Service Providers and customers and explains how cloud security training and certification can help organizations protect data and meet regulatory demands to ensure data privacy. It also shows individual cybersecurity practitioners how cloud security training and certification can expand their influence and grow their careers.

THE PARADOX OF CLOUD SECURITY

The number of cloud (and overall cybersecurity) data breaches is rising precipitously. During the first six months of 2019, data breaches increased by 54% compared to the same period in 2018.[1] Nearly 31 million records were exposed in the 13 biggest data breaches[2] alone.

Yet, cloud security today is better than ever. A report from McAfee[3] found that 52% of companies surveyed experienced better security in the cloud than in their on-premises data centers. After all, Cloud Service Providers see more attacks than most companies ever will and thus gain more experience fending off assaults. As Thomas Stowassaer, Architect Manager of Microsoft Secure explains, "We have specific teams that go after attacks and they see far more hacks than most companies do. We learn from these attacks and make corrections to mitigate them. That gives us a level of security customers couldn't have on their own."

Thanks to their massive scale, public Cloud Service Providers such as Amazon Web Services, Microsoft Azure and Google Cloud Platform also have the resources to hire large teams of security experts and to invest in the latest and most effective technologies. Most customer organizations, even the very largest companies, are unable to duplicate these efforts.

If cloud security is better than ever, how do we explain the ever-increasing number of data breaches?

> "Cloud Service Providers are concerned with keeping up with zero-day vulnerabilities and data exploits. We pay considerable attention to patching systems to make sure vulnerabilities don't lead to unnecessary exposure."
>
> - Olayinka "Olay" Ladeji, Senior Principal Program Manager, Cloud Operations

The disconnect comes from the fact that the cloud uses a Shared Security model. Cloud Service Providers protect the datacenter. But customers are responsible for safeguarding their own data. As Jay Heiser, vice president and cloud security lead at Gartner, Inc. explains in CSO Online[4], "We are in a cloud security transition period in which focus is shifting from the provider to the customer." A survey by McAfee[5] illustrates the point. It found that only 36% of vendors can currently enforce data loss prevention (DLP) in the cloud and only 33% can control how users collaborate and share data in the cloud.

CLOUD CUSTOMERS MUST TAKE CHARGE OF DATA SECURITY

Cloud customers are thus left to fend off the wide range of security threats that currently imperil customer data in the cloud themselves. The most significant of these threats include insufficient access management and account hijacking, system misconfiguration, hyperconverged environments, insecure interfaces and APIs, and emerging threats.

Insufficient Access Management and Account Hijacking

Cybercriminals posing as legitimate users, operators or developers can read, modify and delete data, perform system management functions and more. These bad actors gain access to systems through weak authentication or through social engineering tactics like phishing that enable them to steal legitimate user credentials. According to the Verizon 2019 Data Breach Investigations Report, 32% of data breaches involve phishing.[6]

System Misconfiguration

Cloud customers also expose data through system misconfiguration. A recent Cloud Security Alliance report, "Top Threats to Cloud Computing: Deep Dive"[7] noted that system misconfiguration is one of the top three threats facing cloud platforms. A TechRepublic study found that misconfigured databases and services have resulted in the exposure of more than 3.2 billion records so far in 2019.[8]

> "Because CSP data centers are secure, we're seeing hackers moving to cloud tenants and stealing identities. When hackers steal passwords, they can misuse cloud tenants and steal data."
>
> Thomas Stowasser,
> Architect Manager for MS Secure

Hyperconverged Environments

Cybersecurity is only as strong as its weakest link. Hyperconvergence is an IT framework that combines storage computing and networking into a single system. As customers increasingly create hyperconverged systems, where applications and data housed in relatively insecure on-premises data centers are integrated with cloud-based systems, data risks grow because they now have more computing power and capability that's just as vulnerable as in their on-premises systems.

Insecure Interfaces and APIs

Many cloud providers expose APIs that customers can use to manage and interact with cloud services. When these interfaces are not protected, they present a risk. These interfaces need to incorporate security to protect against accidental and malicious attempts to circumvent policy.

Future Threats

Threat actors are starting to use artificial intelligence and machine learning to enhance their abilities to deliver, scan and even develop new cyber weapons. A survey by Webroot[9] found that 91% of cybersecurity professionals are concerned about hackers using AI against companies in cyberattacks.

91% of cybersecurity professionals concerned about hackers using AI against companies in cyberattacks.

CLOUD CUSTOMERS NEED A STRATEGIC SOLUTION

Cloud users today must take responsibility for minimizing the risk of data breaches in the cloud. Not only is ensuring good data security critical to their relationships with their customers, organizations must also adhere to a growing list of regulations that require them to protect data privacy and keep customer data secure. These regulations include the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA) and many others.

Yet, many organizations are held back in this effort by a lack of strategic focus. Says Luis Gonsalves, Head of Security for Banco de Portugal, "Many companies begin their cloud adoption journey without properly thinking about security first and having an architecture, strategy and vision in place. From a leadership and strategic perspective, that's one of the biggest challenges and will create additional risks for these companies."

ENABLING A COMPREHENSIVE CLOUD SECURITY SOLUTION

To create a Secure-by-Design cloud strategy, organizations need a comprehensive understanding of the cloud's unique benefits, architecture and risks. In particular, they need knowledge of:

» Cloud benefits, including rapid time to market, scalability and flexibility

» Essential characteristics, service models and deployment models of cloud concept architecture

» Unique cloud risks, such as the shared security model

» Available security architectures and strategies and when to apply them. For example, industry analysts increasingly recommend that companies adopt zero trust architectures with micro segmentation to ensure that each cloud resource is protected, reduce the attack surface and prevent lateral movement of threats across the environment

» The types of technical security controls necessary to mitigate cloud risks

» How cloud security controls map to current and upcoming data privacy regulations, such as GDPR, CCPA and HIPAA

» Legal contract terms in agreements with Cloud Service Providers that map out responsibilities

THE IMPORTANCE OF CLOUD SECURITY TRAINING FOR ORGANIZATIONS

Cloud security training and certification programs can ensure that organizations have in house experts with a comprehensive understanding of cloud benefits, architectures, risks, best practices and controls, as well as the ability to communicate between IT and business staff.

A Strategic Understanding

Many cybersecurity experts have expertise in one or two areas, but they don't understand how to bring everything together to create a comprehensive cloud security posture. A good training program provides a strategic overview of cloud benefits, architecture and security. Training can also provide a taxonomy and definitions of terms to reduce confusion and help people better execute the mission because they're all speaking the same language.

> "A good cloud security training program can provide a comprehensive overview of cloud technology, help organizations formulate an appropriate use case, as well as select cloud deployment, implementation and service models to address that."
>
> Dr. Lyron Andrews, authorized (ISC)^2 instructor

Cloud Risks and Mitigations

The cloud has unique risks. "Training classes expose students to those risks and how to handle them," says Ben Masilow, authorized (ISC)^2 instructor. "They talk about proper planning and policies, incident response methodologies and techniques so that companies can reduce risks and meet regulatory requirements."

Best Practices and Hands-on Experiences

Organizations need a cloud environment that is Secure by Design. Training can introduce organizations to best practices they can build upon and technologies they can use to build a secure environment. A mix of practical exercises and discussions of real-world problems demonstrate how concepts apply to an organization's use case. Most importantly, training can deliver platform-agnostic, independent perspective overview of technologies and solutions.

Mapping Technology to Regulatory Requirements

To help organizations address regulatory requirements, training courses can map the top cloud security frameworks and controls to the requirements in individual regulations that are relevant to a business.

Explaining Contract Terms

The cloud is a managed third-party service. It differs from traditional environments in that the customer is no longer responsible for their own IT. Thus, the contract is paramount for spelling out who is responsible for what and what the customer is permitted to do (such as penetration testing). “Many good IT and security practitioners aren’t familiar with crafting contract language or with what contract terms they should be asking for. Training can give them insights they wouldn’t have had otherwise,” says Masilow.

Facilitating Communication Between Business Users and IT Professionals

Technicians need to speak the language of executives and business users to truly address cloud security concerns. “Training solutions teach cloud security technicians to speak the language of business by talking about the IT infrastructure library (ITIL),” says Andrews. “ITIL is a way to talk about services, not technology—and data, not infrastructure—encouraging technicians to have a business mindset.”

CAREER ADVANCEMENT FOR THE INDIVIDUAL CLOUD SECURITY PRACTITIONER

While providing benefits for the organization as a whole, cloud security training also pays big dividends for individual security practitioners. Overall, the market is very good for general cybersecurity practitioners; 57% of organizations plan to hire cybersecurity staff in the next year, according to eSecurity Planet's 2019 State of IT Security[10] survey. Yet organizations are stymied by a global cybersecurity staffing shortage of roughly 3 million.[11]

Cloud security is one of the cybersecurity areas where professionals are in greatest demand. More and more organizations are using cloud services, moving some of their operations to the cloud or offering cloud-native applications that may span their own data centers and public clouds.

Training qualifies security experts for these cloud security jobs by providing:

28%

The year-over-year growth for cloud-related job postings across all of the online recruiting sites, such as Indeed, Dice, Career Builder, Glassdoor and Simply Hired.

Mentorship

Instructors generally have decades of experience and world-class credentials while classes put together the right body of knowledge and explain cloud security in a comprehensive manner. Nanditha Rao, Information Security Senior Advisor explains that her cloud security training, "provided experts to explain the concepts and help me understand the level of abstraction the cloud offers."

A Respected Credential

Clients and employers want assurance that a security professional knows the key industry trends. "Certifications like CCSP (Certified Cloud Security Professional) benchmark cloud security proficiency," says Olayinka "Olay" Ladeji, Senior Principal Program Manager, Oracle Cloud Security at Oracle America. Certification also helps employers find security practitioners. "A lot of human resources organizations use keyword searches, so certification helps candidates stand out," says Masilow.

Access to Outside Expertise and Resources

Individual security practitioners cannot be experts in every aspect of cloud security. Certification and training programs promote networking so practitioners can find individuals with complementary knowledge. "There's a lot of cross pollination," says Masilow. "There's always someone in class who knows about areas you might need help with. Classes also make individuals aware of useful resources, such as free NIST documents, CSA guidance or the CCA's Cloud Control Matrix."

A Seat at the Table

With the expertise gained from training and certification, professionals gain the strategic knowledge to help guide their organizations' overall security policy.

> "With CCSP certification, I can now provide my input into the design and migration discussions at the enterprise level."
>
> Nanditha Rao, Information Security Senior Advisor

CCSP℠ | Certified Cloud Security Professional

A Good Salary

The shortage of cybersecurity professionals, and cloud security professionals in particular, has resulted in high salaries. The average salary for a certified cloud security professional is $134,000.

Career Growth

Most importantly, CCSP training and certification enables security professionals to achieve career success. As Ladeji notes, "Since I've had my CCSP certification, I've moved up and switched roles, so I do more in terms of level and salary."

CONCLUSION

Organizations today need both a strategic and tactical understanding of cloud architecture and security if they are to protect their data from breaches and comply with a growing number of data privacy regulations. Cloud training and certification programs, such as CCSP, give organizations the comprehensive understanding they need to truly safeguard their customers' sensitive personal data—and enable security professionals to meet their organization's needs while growing their careers. ■

The CCSP certification shows you have the advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by the cybersecurity experts at (ISC)².

Interested in the CCSP? Get the Ultimate Guide to the CCSP and discover the pathway to certification.

[1] "The 13 Biggest Data Breaches of 2019 (So Far), CRN, July 16, 2019, By Michael Novinson

[2] https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/

[3] https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-cloud-adoption-risk-report-business-growth-edition.pdf

[4] https://www.csoonline.com/article/3043030/the-dirty-dozen-12-top-cloud-security-threats.html

[5] https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-cloud-adoption-risk-report-business-growth-edition.pdf

[6] https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

[7] https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-deep-dive/

[8] https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/

[9] https://www.webroot.com/us/en/about/press-room/releases/cybercriminals-using-ai-in-attacks

[10] https://www.esecurityplanet.com/network-security/survey-2019-businesses-accelerate-spending-hiring.html

[11] https://searchsecurity.techtarget.com/news/252450942/ISC2-Cybersecurity-workforce-shortage-nears-3-million-worldwide

[12] https://resources.infosecinstitute.com/category/certifications-training/ccsp/ccsp-job-outlook/#gref

[13] https://resources.infosecinstitute.com/category/certifications-training/ccsp/ccsp-job-outlook/#gref

(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, programmatic approach to security. Our membership, more than 140,000 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 public through our charitable foundation – The Center for Cyber Safety and Education™. Visit www.isc2.org.

CYBER
THEORY

We are a full-service cybersecurity marketing advisory firm. We constantly collect and analyze the latest customer data segmented by security practitioner, industry, and region. Our extensive knowledge model allows us personalized targeting of each and every cybersecurity buyer persona.With strategic insights from global education services, media providers, intelligence analysts, journalists, and executive leaders, we're always adapting to the latest industry trends. Our network of relationships encompass all aspects of cybersecurity as well as the related fields of fraud, audit, compliance, and risk management.

(212) 518-1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018 • www.cybertheory.io