CCSP Certified Cloud Security Professional

WHITEPAPER

# The Rise of the Cloud Security Professional

## *An Emerging Voice Within IT and the Business*

## Executive Summary

The growing sophistication and prevalence of cloud technology is giving rise to a new type of IT specialist: the Certified Cloud Security Professional (CCSP℠). This is an individual with demonstrated experience and competence in information security and cloud computing, who parlays that background into an advanced vocational designation that delivers both the practical and strategic knowledge required to help organizations benefit from the power of cloud computing while keeping sensitive data secure.

Increasingly, this type of person is needed in the boardroom, and not just in front of a computer screen. The use of cloud technology is central to every aspect of a company's existence, and the strategy to deploy it effectively requires a clear and experienced voice.

This paper looks at the relationship between IT and the C-suite, and through case studies and a discussion of the role of risk in corporate management, requires a role for the CCSP as a key player on the strategic forefront of a company's life.

## Cloud Security and the C-Suite

The use of the term "cloud" to describe the global collection of interconnected servers and computers as a strong symbol of its amorphous and ever-expanding nature, illustrates the way it seems to hover above us, allowing information to be pulled down to wherever we happen to be. However, there is a parallel and less comfortable analogy that IT security professionals know only too well, and that anyone who has ever flown in a plane has also experienced literally. This is the sensation of flying headlong into an actual cloud, in which visibility is zero, and where you find yourself hurdling headlong into the unknown at 600 miles an hour. This, in a way, is what cloud security specialists face every day and, so too, do the rest of us, travelling ever forward into seemingly misty nothingness.

Security inside the cloud is a never-ending and ever-growing challenge. Those in charge must be a special breed: technically competent, eternally curious, ruthlessly organized, and politically aware. This is a tall order, since the tradition of IT has always been something of a mysterious back-office operation. In many companies, for many years, the IT department, and the security organization in particular, was looked upon as something of a hindrance – something that got in the way and which held an obscure position within the corporate hierarchy.

Today, however, the cloud is inextricably linked to all components of a business: customer-facing, within teams and departments, out on the road with the sales force, and in the back office. As such, senior managers are starting to recognize the need to offer IT and security a seat at the C-suite table. Although the cloud is overall a revolutionary approach to conducting business, it comes with risks and, to that end, sound wisdom and experience are needed, the type that only cloud security professionals can provide.

For some organizations, the battle to provide the additional seats at the C-level table is one fought on two fronts. Traditionally executives saw IT as a niche department, responsible for ensuring that the computers were working okay, and at the same time IT professionals kept to themselves, unwilling, or simply too busy to interact on a strategic level when there were fires to put out. But in recent years, many executives have become more aware of the direct impact of the digital world, and they continue to work hard to steer their companies into the cloud environment, as well as related subsets such as digital commerce and social media. To match this, IT professionals, including security specialists, find themselves in need of a complementary skillset: the ability to talk strategically and negotiate with senior-level decision makers.

## Trust but Verify

The challenge with implementing a secure cloud strategy is that there is often a lack of understanding around how to define cloud computing and its risks. Adam Gordon, CCSP, an author and instructor for (ISC)[2®], puts it like this:

> "There has been great interest over the last several years in anything and everything cloud. The problem is we don't always understand what cloud means, we don't always understand what it may mean as we start to consume as individuals and as businesses and, as a result, there tends to be a gap, where consumption is a lead indicator and security is an afterthought."

Organizations and their leaders need to be fully aware of the extent of the cloud's reach into their organization. For example, when an individual uses a smartphone to check on directions to a meeting, that person is using a cloud service. But, Gordon asks, are they doing so securely?

> "As individuals, do they understand the implications of allowing the application on their phone – the map application, to be able to locate you and provide that location information to a cloud service? How is it being used? How is it being archived? How is it being tracked? As businesses, we have to wonder about individuals consuming information through the cloud. Is that information being transmitted securely? Is it stored securely? These are grave concerns for individuals and businesses."

Innocent actions such as using a smartphone's location app or even using cloud-based file storage or file transfer services can easily turn a "pinhole in a dam" into a raging torrent. Collectively, a company's employees put faith into their cloud provider and say, "they're going to take care of it," without stopping to verify. Gordon refers to a phrase used by President Reagan during the 1987 arms control negotiations, taken from a traditional Russian proverb: trust but verify. "If you take the trust but verify approach, we come up with a solution that actually leads to cloud security. If we just trust, but don't verify, I think we're in for some nasty surprises along the way."

Cloud security must instead become a true partnership between the cloud provider, the cloud consumer, and the people and machines touched by those two parties as they interact with cloud services today. Corporate customers, including all levels of the executive suite, need to be actively involved in cloud security by becoming better educated and understanding how to consume securely, and not just assume everything will be okay.

## Cloud Security as a Component of Risk Management

Risk is the language of the C-suite. Executives spend much of their time identifying the risks faced by their organization and then devising strategies for risk management, abatement, and awareness. As such, a vector of questioning opens up around the risk inherent in cloud technology.

One of the many responsibilities of the cloud security professional is to become the arbitrator of these executive-level conversations around security in the world of cloud computing and the interconnecting cloud solutions.

Organizations need a defined set of policies and processes that team members at all levels can depend on. Many cloud security professionals will readily attest that one of the biggest issues they face is the idea of how to create this common ground in terms of what needs to be discussed, and to frame the executive conversation around risk, liability, security, and related topics.

Specifically there is a bias among many at the executive level that the public cloud is not sufficiently secure, and that keeping data stored in-house is the better route. It feels better to be able to look at the servers and

computers that exist inside a company's own walls and believe that the data is locked in.

Dale Vile, research director at IT analyst firm Freeform Dynamics, points out in CIO.com how many of the fears felt by executives stem from uncertainty or emotion. "They worry about their data being stored together with everyone else's, and fret over what they see as a loss of control over their information assets. Mixed up in all this are issues of trust - they are often concerned that the provider will abuse their data, especially when it comes to public cloud. When you press them, however, people with less experience often struggle to articulate their concerns in a meaningful way. What often comes across is a general fear of the unknown." [1]

Executives also fear the notion that their company's data is under someone else's control – an external provider that may or may not remain in business. Further, there are compliance issues to wrestle with – including the physical location in which data is stored, and even which countries it may pass through when being transmitted. These are complex issues that actually go beyond the data being stored and moves into legal territory.

Cloud security experts are quick to point out that external cloud providers make it their business to stay secure and up-to-date. It does not mean external providers are 100 percent foolproof, but they tend to spend much more time and resources in keeping things tight and secure. This is important when compared to the actions of employees inside a typical company – who use unsafe Wi-Fi connections, practice poor password management skills, click on phishing emails, or leave laptops or USB drives behind. Recent famous breaches bear this out.

- When the Sally Beauty chain of beauty products was hacked in March 2014, resulting in the loss of 260,000 credit card numbers, security analysts discovered that the hackers had gained access through the login credentials of a district manager, whose laptop had his username and password taped to the front of it. [2]
- The 2014 breaches at Home Depot and Target were each the result of hacked third-party vendors who had been given access to the companies' networks. [3]
- The infamous Ashley Madison breach of 2015 has been thought to have been an inside job – the product of a disgruntled employee – a theory suggested by security entrepreneur John McAfee. Regardless of whether this theory bears fruit, the key lesson from Ashley Madison is that the data, although well encrypted, was stored in a single location, making it easy to download. [4]

Breaches and hacks happen to companies every day. Cybercriminals exhibit a drive and perseverance that is relentless, and their sophistication is growing. The assessment, understanding of, and containment of this type of corporate risk requires a specific combination of attention to detail paired with experience. This combined skillset needs to be present in a company's security specialists.

## Diplomacy, Politics, and Language

Any security system is only as good as the people who use it day-to-day. As such, cloud security experts seek to remind their clients that when performing internal audits of company systems, it is not enough to simply audit the outcomes of what they are configured for; companies must audit the process to make sure that people are doing things in a way that consistently reaches management's expected outcomes. This extends the spectrum of security from an exclusive focus on technology to the awareness of humans and human nature.

To achieve this level of security, IT professionals need a forum for their recommendations and worries. They need to be able to speak frankly at the executive table, but also to educate members of senior management in real time, in the trenches and on the front lines. Adam Gordon adds:

---

[1] Trotter, Paul. "Top Cloud Security Fears & How The C-Suite Is Tackling Them" (May 20, 2015) http://www.cio.com/article/2924390/cloud-security/top-cloud-security-fears-and-how-the-c-suite-is-tackling-them.html

[2] Krebs, Brian. "Deconstructing the 2014 Sally Beauty Breach" (May 2015) http://krebsonsecurity.com/tag/home-depot-breach/

[3] Krebs, Brian. "Deconstructing the 2014 Sally Beauty Breach" (May 2015) http://krebsonsecurity.com/tag/home-depot-breach/

[4] Smith, Matt. "McAfee Has an Interesting Theory about the Ashley Madison Hack" (August 2015) http://www.digitaltrends.com/computing/john-mcafee-says-the-ashley-madison-hack-was-an-inside-job

> "I ask my customers all the time, 'Have you walked around the business recently? Have you done what a normal worker in your world does, even just for a minute? Or for an hour? Or a day? When was the last time you acted not like a senior executive but like a normal team member in your organization?'"

Seeking these answers requires a cultural translation from the facts and figures that IT people are most comfortable with, to a clear connection with senior-level corporate priorities. Andrew Wild, CSO of network, cloud security, and legal compliance software provider Qualys, points out that the risk-based approach preferred by C-level management means security leaders must:

> "Move away from a security controls focused approach to information security. [...] A critical component of implementing a successful risk-based approach is building strong relationships with business units, approaching them in a consultative manner to offer assistance and guidance. [...] Having the security controls mapped to the risks they are designed to mitigate can bring more transparency and understanding to the information security budget." [5]

In other words, security issues must be framed in strategic language in order to be heard. Wild continues by pointing out a specific situation:

> "Security chiefs often present detailed charts with metrics explaining the effectiveness of security controls. [...] The C-suite and board need to understand how well the organization's risk management program is functioning, and a chart that indicates how many malware incidents were identified and remediated over time may not be the right metric to share. Instead, provide information about the effectiveness of the processes through which risks are identified. Explain how risks are measured, qualified, or quantified. Describe the processes that identify and implement effective controls for risks, and for periodically assessing how effective these controls are."

This is the language of executive-speak. It generally maintains higher-level vision and longer timelines. Qualified security experts must embrace this culture and become fluent in it.

## The Ever-Growing Risk

Most organizations already have a Chief Information Officer and/or a Chief Technology Officer. It can be easily assumed that this individual can take care of the senior-level strategizing and risk management for all technology-related aspects of an organization; but it is not always possible for such a person to know all of the dangers and have all of the solutions. This is why specialists exist and must be invited to the discussion. The existence of the OWASP Top Ten highlights this need.

The Open Web Application Security Project (OWASP) is a non-profit organization that focuses on software security. It regularly publishes the OWASP Top Ten, a summary of the ten most critical web application security flaws. The list analyzes these flaws for damage potential and the degree of work required to rectify the problem. Its current top ten includes threats such as SQL Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), Unvalidated Redirects and Forwards, and five others. Each of these ten flaws is severe enough to allow attackers to take over a company's site, and two of them, "Security Misconfiguration" and "Using Components with Known Vulnerabilities," are actually considered "out of scope," meaning they cannot be rectified with normal procedures or tools.

This means an internal security team will have its hands full trying to figure out what to do with just the "out-of-scope" challenges, let alone the other eight threats. These threats continue to change shape and advance in sophistication. Focusing solely on these two items distracts

[5] Zetlin, Minda. "Chief Security Officers are Gaining C-Suite Acceptance." (May 15, 2014) https://enterprisersproject.com/article/chief-security-officers-are-gaining-c-suite-acceptance-qa-andrew-wild

the security team from the other challenges inherent in keeping a network and business safe. This requires the expertise of both internal and external security personnel. There are too many new types of attacks for any one individual to manage. The CIO and the rest of the executive suite need competent security professionals to handle them, and also need these individuals to communicate the threats and the plans for detection and avoidance in a language most comfortable for non-IT employees.

This gives rise to the need for a specific type of credentialed professional – someone who has the front-line expertise to understand the multifaceted nature of cloud security and the political ability to express it credibly.

As (ISC)$^2$ CEO David Shearer states:

> "Communication is critical. Credentialing and standards related to credentialing can create a common lexicon for communities of interest to collaborate and converge on complex topics. It helps drive business cases forward to the C-suite, to help get them the funding streams that help them get the resources they need."

## How to Instill a Proactive Security Mindset

A proactive mindset is in fact an unnatural thing. Human beings are hard-wired to react to danger, but anticipating it and taking action to offset it is a learned skill, and one that often comes after a crisis, not before. People resist spending money on invisible dangers, and this poses a significant challenge to the IT security organizations, given that the dangers that appear on their radar are numerous, and increase by the day.

Security professionals and senior management need to steer away from the state of denial that plagues many businesses. Some believe they are too small to be noticed, while others feel they are too large to be threatened. Both assumptions are wrong. To choose just one example out of many, an attack that paralyzed the main websites of Capital One, HSBC, and a number of U.S. banks in 2013, was discovered to have originated in Turkey, but had been funneled through a completely innocent general interest online store based in the UK. This store's website unleashed an army of zombie bots that repeatedly attacked the banks' websites in a technique known as Distributed Denial of Service (DDoS). San Francisco-based security company Incapsula detected the attack early and was able to shut it down before major damage occurred, but as Incapsula security analyst Ronen Atias wrote in his account of the event, "this is just another demonstration of how security [on] the internet is always determined by the weakest link." He points out that the simple mismanagement of an administrative password on the UK website was quickly exploited by the botnet shepherds in Turkey. "This is a good example," he says, "of how we are all just a part of a shared ecosystem where website security should be a shared goal and a shared responsibility." [6] Incapsula CEO Gur Shatz agrees:

> "In general, hackers are lazy and will almost always take the easiest path to infiltrate their target. The fact that an alarmingly large number of incidents involve simple password theft indicates that this is still a major issue. [...] When assessing a company's risk for exposure to APTs, it is common for some to take a head-in-the-sand approach, thinking, for example, 'I'm not a bank, I make farm equipment, so I do not have to worry.' But Shatz points out a company without any major secrets or critical online functionality is still subject to being used as a "mule" to conduct cybercrime." [7]

The need for vigilance is paramount. The cloud continues to grow in size, variety, and sophistication. Added to this is the explosion of connection points represented by the Internet of Things (IoT), in which devices ranging from coffee pots to trucks, and even herds of cows, will communicate, device to device, sharing data and penetrating companies systems, ostensibly in the name of improved service to the customer. The permutations for abuse become infinite.

[6] http://www.incapsula.com/the-incapsula-blog/item/603-cyber-attack-us-banks

[7] Prentice, Steve. "Dark Clouds on the Horizon: The Rise of Sophisticated Cybercrime" (October 2013) http://cloudtweaks.com/2013/10/dark-clouds-on-the-horizon-the-rise-of-sophisticated-cybercrime

## The Difference Between Proactivity and "The Sky is Falling"

There is a difference between maintaining a proactive corporate mindset and simply believing in a gloom and doom scenario, and this relies on clear planning, clear communication, and sufficient on-going education. A CCSP-certified cloud security expert interviewed for this paper on the condition of anonymity exclaimed that one of the largest challenges faced involves "not knowing what you don't know:"

> "Because cloud is such a young environment, if there is a threat to the hypervisor that runs a virtualized environment, it may not even be detected yet or, if it is, I may not know about it, and that threatens my integrity because I am the provider, so it also threatens my customer's data, and that is not funny at all. Since I am the one running the hypervisor, I had better know about that stuff. So we try to keep up-to-date with everything that is out there, but it is what I don't know that scares me."

David Shearer compares this to specialized medical detective work:

> "We are getting better at determining compromises and breaches. I equate it to looking at cancer years ago. We were unable to find cancer in people as readily as we are today, but now we are consequently finding more cancers. I tend to look at bad actors and exploits of technology as a cancerous type of activity, and as we get better at detecting, we are finding more. We used to have the sense that our data was in the data center within a corporation, and now the data is peppered around the planet on all types of mobile devices; and these devices provide attack vectors and pivot points with which to exploit an organization. I see that our attack surface is growing, and the numbers of attacks are increasing; and we don't see any trending off."

Clear and regular input from vendors, industry watchdogs and colleagues allows for the creation of a real-time knowledge base from which IT security experts can extrapolate instructions, policies, and procedures. It is then up to senior management to accept and implement these procedures without falling prey to complacency or the temptation to trim budgets and staff.

## The Need for Credentialed Cloud Security Professionals

Cloud security exists to address a clear and present, and ever-growing danger. To handle this effectively and to communicate messages and advice requires naming conventions that lead to clear conversations. Frequent communication is critical.

By employing credentialed cloud security professionals, companies can ensure they are using the recommended best practices, security standards, and common lexicon that will create and maintain secure cloud computing infrastructures. Although many people can claim to be experts in IT security, current technological and political ecosystems do not allow for security techniques to be learned on-the-job. Companies require professionals who have already had years of experience in IT security, including cloud security, in order to hit the ground running. Although there is always more to learn, an established skillset is essential from the start.

Organizations are now turning to respected industry credentials, specifically the Certified Cloud Security Professional (CCSP) certification, to ensure that cloud security professionals have the knowledge, skills, and abilities to audit, assess, and secure cloud infrastructures. This designation requires candidates to demonstrate sufficient experience, specifically five years in IT, three years in IT security, and one year in cloud security. This gives information security and IT staff the skills and credibility to get the job done, and gives organizations greater comfort in granting the freedom and authority needed to confidently move IT infrastructure to the cloud.

But just as companies need credentialed professionals, these professionals have needs too. When asked what their ideal work situation would consist of, many confess to needing more time for the proactive work. As one anonymous expert puts it:

> "You are always behind and you are always firefighting. Not necessarily hacks. The bigger stuff is trying to maintain compliance and a secure configuration amid changing environments. Here is one thing that most

people do not understand: you imagine that you set up all of these servers and they are more or less static. In other words you set them up once and everything is fine, but in reality that is very far from the case. They are rapidly changing environments. Every time there is an update to your operating system, and you are running software, they can change your actual security configurations. You have to constantly go back and review what's going on, scanning your systems, and seeing what vulnerabilities that previously had been closed have been reopened again. That is a constant battle, staying configured correctly."

David Shearer adds a strategic viewpoint:

"There is a certain sense that the workforce can't get their heads above water, due to a lack of processes in place. You almost need a surge of resources to come in and help them get their heads above the water line. There is a powerful need to get user awareness training in place along with disaster recovery and business continuity. They don't get time to work on a lot of these things because they are too busy patching and fixing vulnerabilities and incidents that don't let them get above that. Industry-wide, we need to help raise awareness within the C-suite, that in order to get a program in place, you might need a group of people fixing the things that are broken today, and another group of people that are laying in place the programs that are needed for a response and security structure for your enterprise."

The credentialed cloud security expert delivers a far greater skillset than simply understanding the mechanics of information technology. This is an individual whose strategic knowledge and communication skills translate into an asset for any company interested in moving forward safely.


brought to you by (ISC)² and CSA cloud security alliance℠

For more information about the CCSP credential, visit www.isc2.org/ccsp.

**About (ISC)²**

Formed in 1989, (ISC)² is the largest not-for-profit membership body of certified cyber, information, software and infrastructure security professionals worldwide, with nearly 110,000 members in more than 160 countries. Globally recognized as the Gold Standard, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, as well as the Certified Secure Software Lifecycle Professional (CSSLP®), the Certified Cyber Forensics Professional (CCFP®), Certified Cloud Security Professional (CCSP℠), Certified Authorization Professional (CAP®), HealthCare Information Security and Privacy Practitioner (HCISPP®), and Systems Security Certified Practitioner (SSCP®) credentials to qualifying candidates. (ISC)²'s certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK®, a compendium of information and software security topics. More information is available at www.isc2.org.



Follow (ISC)² on Facebook, Twitter and YouTube.

(ISC)²®