RAPID7

THE CLOUD:
HOW CISOS CAN EMBRACE IT (WISELY), NOT FEAR IT

01 INTRODUCTION

Cloud computing is one of the great transformational shifts in corporate information technology. It allows businesses to manage their IT needs in innumerable new ways—some of them great, some of them terrible.

That last part is what worries chief information security officers.

The truth is that cloud services are already a fixed part of the corporate IT landscape. Businesses have been adopting the cloud for one task after another: customer relationship management; corporate accounting; regulatory compliance; risk management. Microsoft provides its Office 365 software via the cloud to 85 million businesses. Google manages corporate email systems. Adobe offers graphic design services to millions of creative professionals.

> "73% (of organizations) have adopted at least one cloud security component."
>
> – 2016 IDG Enterprise Cloud Computing Survey

More concerning for CISOs, however, is that cloud services have also become a fixed idea in employees' minds—as in, "We need a quick way to get this done. We can just find some cheap provider on the Internet, right?"

Wrong. That is the allure of the cloud's ease-of-use running roughshod over its risks. It is precisely what CISOs need to prevent. Part of your role must be to develop a security plan that includes the cloud; rather than one that ignores it. If you don't, you will be in the position of responding to employees pushing for security reviews during the procurement process—or worse, during deployment. You want to be showing them the way forward.

CISOs can't fault operations and finance executives for wanting to embrace the cloud. Using cloud services does cut investment costs and relieve the IT team of tedious chores. The functionality of the applications often is better than what coders could develop in-house. The business case for using cloud services is compelling, and it will only become more so in the future.

That said, CISOs have a different priority. Your role is to guide and govern the business functions driving daily operations at the company. When the business units see a breakthrough in technology that can help them do their jobs (and cloud services do qualify as such), the CISO's job is to help other parts of the enterprise harness the power of that technology effectively.

If not—if a CISO categorically opposes the use of cloud services—then employees will quickly come to see the security function as an obstacle: something to be tolerated at best, and evaded when necessary. A CISO never wants to be in that position. You want to be perceived as someone who enables the business units do their jobs well, and they will see using the cloud as part of that.

To embrace the cloud fully and wisely, then, a CISO needs to master two roles.

To embrace the cloud fully and wisely, then, a CISO needs to master two roles. First, he or she must participate as part of the team that evaluates cloud providers—bringing the proper security expertise to the finance and business executives eager to use the cloud. Second, the CISO must also know how to evaluate the security of cloud services.

Let's take each point in turn.

02 HARMONIZING THE THREE VOICES

All decisions to use the cloud will be driven by three voices within your organization: the operations team that has a specific need it wants to solve via the cloud; the finance team that wants to weigh the costs and savings; and the security team concerned about risks.

CISOs need to respect that dynamic and help to guide it wisely. That means the company should have a structured process to govern when and how employees use cloud services—not something ad hoc that might change depending on the people debating the question, or the particular idea on any given day.

For example, does the company have a written policy that governs how, and for what, employees can use cloud services? Is that policy clear? Does it reflect a practical assessment of the company's security risks? Has that policy been communicated to the workforce, and are you sure they understand it?

That preliminary spadework can make subsequent discussions about using cloud services go much more smoothly. Again, the risk isn't that the company uses the cloud at all; the risk is that some small pocket of the organization uses the cloud unwisely, because that small pocket doesn't know how to evaluate all the factors your organization should consider before moving to the cloud.

Another way to underline the importance of a good process is to consider how your business might move to the cloud without one.

In that world, the operating unit can become the dominant voice pushing the conversation because it wants the ease of cloud services so much. The CISO ends up becoming the final arbiter of whether to use any cloud, rather than an early advisor on how to use the cloud. Business units may come to view the security team as "the enemy" trying to thwart their plans. They might even take the riskiest action of all: using the cloud without telling you.

> The risk isn't that the company uses the cloud at all; the risk is that some small pocket of the organization uses the cloud unwisely...

That is not at all where a risk adviser wants to be.

That's why a thoughtful process for using cloud services is so crucial. It lets the CISO be a bridge between the business and the cloud, so they can have a productive conversation about what will work best for your organization.

So how does that thoughtful process unfold? Once the business does decide to use cloud services, how does the CISO evaluate each solution's security posture and determine what's a good fit for your organization?

That brings us to the second skill a CISO needs to master.

03 ASKING THE RIGHT QUESTIONS

Your goal when assessing the security of a cloud solution is to determine how it handles security and whether that approach makes the provider a good potential partner for your organization.

That is not the same as determining a firm's precise security posture. The service provider might have security protocols ideal for your needs today—but key personnel might leave tomorrow; or the firm might change policies next week; or a new software update might pose unforeseen risks to your data next month.

While you certainly need to collect a lot of information and ask some pointed questions for a thorough evaluation, it's helpful to start the assessment with simple open-ended questions that illuminate the provider's approach to security. Here are some suggestions.

Who is in charge of security? You want to find the highest-ranking person at the provider whose sole job is security—not a vice president of security and IT, who might also oversee tech deployment; not a chief technology officer, who might dabble in strategy. You also want to know how many people directly report to this person, and how large the security team is.

The goal is to understand how the provider "staffs out" security, irrespective of the particular person overseeing the function today. You want assurance that the provider has a structure for security even as personnel change over time.

How does the provider use two-factor authentication? Not only do you want to see where the provider uses 2FA in its product; you want to understand how the provider uses 2FA across its whole operation—including where the company does not use 2FA. (Specifically, is there any point where the provider is transmitting your data without using 2FA?) Does a provider need to use two-factor authentication at every moment? No. The point of the question is simply for the provider to explain its logic, so you, the CISO, can evaluate that logic.

How does the provider govern access control? This question drives at how the provider manages the human factor: people accessing your company's data. How quickly is user access turned on and off, as employees come and go? Does the provider follow Principle of Least Privilege and terminate access even for current employees who no longer need your data? Will outside parties working with the provider also have access to your data?

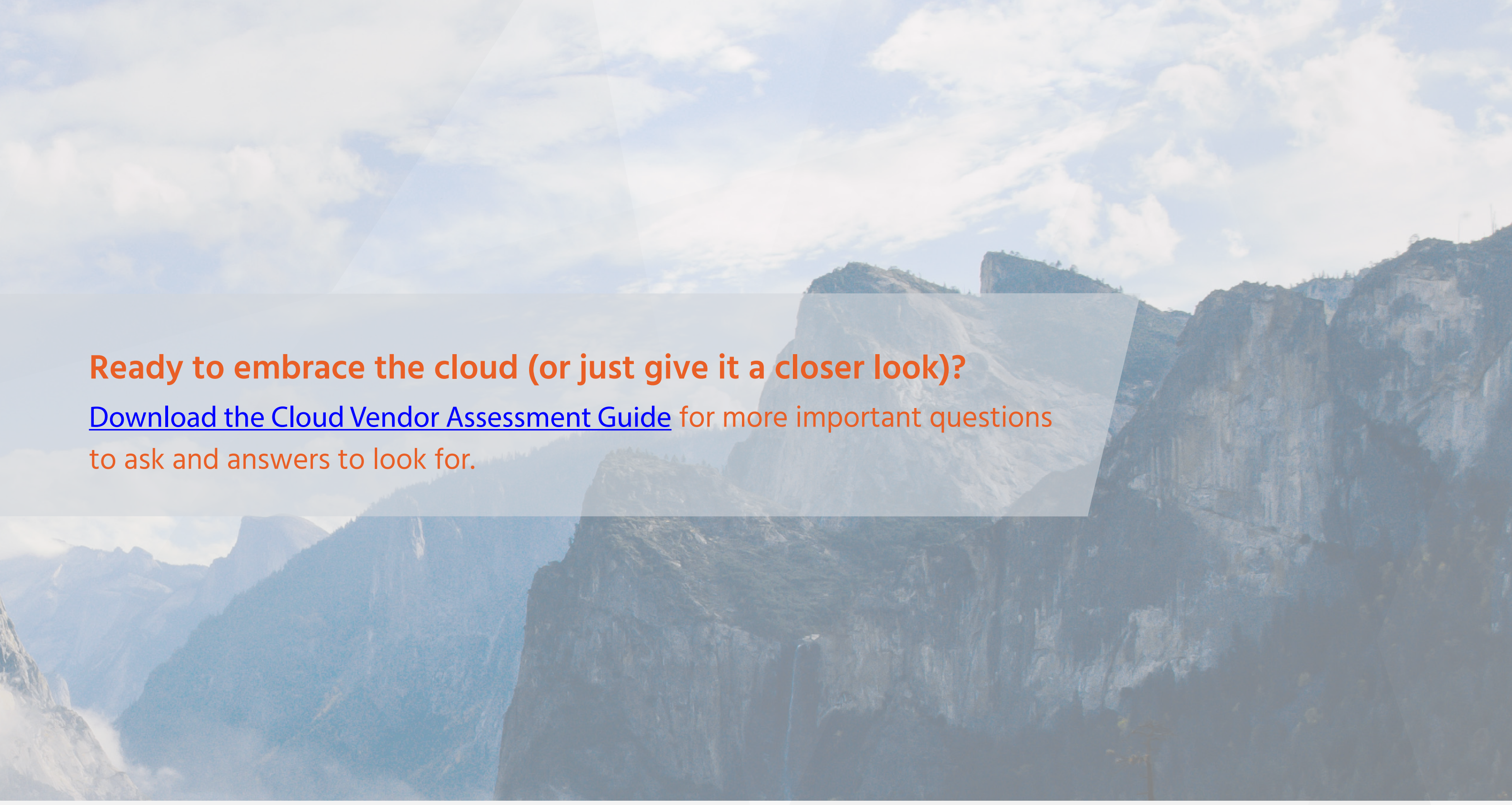
How does the provider assure it has no exposure to known vulnerabilities? Discussions about patch management, vulnerability assessments, application controls—they all demonstrate the provider's awareness of how to handle various threats. Again, there is no single correct answer; what may be crucial to another customer might be irrelevant to you, and vice-versa. You only want to elicit the provider's rationale for policing against threats in the way that it does.

What's the proof? Every reputable cloud services provider will have some outside attestation of its security; the question is whether that attestation is helpful to your company specifically. For example, if the provider had its security audited in a SOC report, did that audit examine procedures relevant to your needs? Or if the attestations didn't, will you be allowed to perform your own testing?

Leadership, multi-factor authentication, access rights, vulnerability management, audits—they are the subjects of conversation a CISO wants to have with a solution provider. Depending on those first answers, demonstrating a provider's security philosophy—then you may want to follow up with pointed questions. Much more important, however, is the broader canvas against which those details are painted.

Above all, CISOs should understand what cloud service providers fundamentally are: an outside contractor who provides a service more efficiently than you can manage yourself. In that respect, they are no different than a cleaning company that provides janitorial services or a landscaping firm that keeps the office grounds neat. They do jobs more efficiently than people in your organization could do themselves.

The cloud can accelerate productivity. Employees will want to use it. The job of the CISO is to advise them on how to use the cloud without putting the company at risk. And with a shrewd, considered assessment of the provider in question, the CISO can do exactly that.



Ready to embrace the cloud (or just give it a closer look)?

Download the Cloud Vendor Assessment Guide for more important questions to ask and answers to look for.

About Rapid7

Rapid7 (NASDAQ: RPD) is trusted by IT and security professionals around the world to manage risk, simplify modern IT complexity, and drive innovation. Rapid7 analytics transform today's vast amounts of security and IT data into the answers needed to securely develop and operate sophisticated IT networks and applications. Rapid7 research, technology, and services drive vulnerability management, penetration testing, application security, incident detection and response, and log management for more than 6,200 organizations across more than 110 countries, including 38% of the Fortune 1000. To learn more about Rapid7 or join our threat research, visit www.rapid7.com.

Rapid7 Insight

Rapid7 Insight is the cloud-based platform that makes it possible—and simple—for security and IT professionals to share data, research findings, and get the answers they need to do their job. The Insight platform significantly reduce overall total cost of ownership inherent with on-premise, analytics-driven solutions, and automatically scales to meet the needs of users, helping to solve challenges presented by rapid data growth for both security and IT.

Rapid7 has been in the security game for nearly two decades, and we understand that moving to the cloud is not taken lightly, by anyone. Our team of developers, engineers, and internal security practitioners have worked for years on the Insight platform to not only reduce your risk and complexity, but also your blood pressure. Processing more than 50 billion events and monitoring millions of assets daily, the Insight platform is the first to unify solutions for vulnerability management, user behavior analytics (UBA), SIEM, IT log analytics, and application security.

Learn more about the Insight platform, as well as the products it supports, at www.rapid7.com/products/insight-platform.