Security is a Partnership

Written by J.R. Arredondo
Director, Product Marketing

RACKSPACE® HOSTING | 1 FANATICAL PLACE | SAN ANTONIO, TX 78218 U.S.A.

rackspace®
the open cloud company

Table of Contents

RACKSPACE® HOSTING | 1 FANATICAL PLACE | SAN ANTONIO, TX 78218 U.S.A.

rackspace®
the open cloud company

1. Introduction

Maintaining a secure environment for applications and infrastructure is a common concern of companies of all sizes. The issue becomes even more important as these companies consider moving their applications onto a dedicated hosted environment or a public cloud. Faced with this situation, organizations may take extreme positions. Let's discuss three of them:

- Some companies perceive the cloud as an inherently unsafe environment that should be avoided at all costs. In doing that, these companies fail to gain the agility, flexibility and other benefits that the cloud provides in the form of a new class of scalable application architectures.
- A second group of companies tries to implement the whole spectrum of security management all by themselves, without benefitting from the experience of the thousands of customers that a cloud provider serves.
- Finally, other companies presume their infrastructure and applications to be secure *just because* they are running on the infrastructure of a third-party provider which, presumably, "takes care of all the security issues."

These extremes represent an overly simplistic view of security management and are dangerous to a company's ability to deliver the services it depends on in a secure manner.

WHY DO SOME ORGANIZATIONS ADHERE TO SOME OF THESE EXTREMES?

Sometimes, business and technical teams fail to engage in deep conversations about the security implications of those projects for their data and applications. Business groups may see Information Technology groups as roadblocks to their business goals rather than as partners. At the same time, it is possible that teams within IT or the Chief Security Office (CSO) may have failed to build communication bridges with their business units to provide visibility over ongoing projects, or may have failed to provide processes that encourage agility within a disciplined security approach. The end result is that business teams are running under the assumption that the provider is responsible for the security of a solution, or think they can handle all issues on their own.

Other times, organizations fail to get into the details of the contractual negotiations with their cloud providers. Sometimes these negotiations are done at high and conceptual levels, leaving lawyers or less experienced personnel in charge of the actual details of the split of responsibilities across company and provider.

More frequently, we see that organizations sometimes adopt a security stance that focuses mainly on technology, or mainly on people and process, without realizing that an effective security management program requires the combination of technologies, disciplines, people and processes.

2. The Increasing Complexity of Security and Compliance Requirements

But the most important reason that organizations struggle with security is that the security landscape is complex. There are three dimensions to this complexity:

- First, there are many **attack vectors and security disciplines**. These include identity, access management, encryption, data protection and trust management, denial of service attack mitigation, vulnerability assessment, end-point security and regulatory requirements, just to name a few.
- Second, there are **multiple layers in a given application's architecture stack**, from the network, systems, operating systems and databases, to the application and its multiple access points. The modern web application is built on multi-tier service-oriented architectures with a myriad of moving parts, and deal with many types of access devices (mobile and desk based). Each one of these layers represents a subset of potential security weaknesses.
- The third is time: **security is an ongoing operation**, not a point-in-time individual project. There is a need for continuous management to maximize the investment one makes in security.

All of this complexity creates the opportunity for specific breakdowns of communication or of operational responsibility.

But the most obvious change in the way application services are delivered is that companies and cloud providers have partial ownership over the whole computing stack of a given service. Sometimes, a cloud provider is responsible for the whole compute stack, as occurs with SaaS applications. More commonly, both the customer and the cloud provider take responsibility over a subset of the application stack. For example, it is possible that the customer manages the application-level components while the provider manages the network and the infrastructure (as is the case in many of our public cloud and dedicated offerings). It is this shared scope over the computing stack that complicates the processes and procedures that must be undertaken to deliver a service that reduces security weaknesses.

3. Security is a Partnership

At Rackspace, we believe that **Security is a Partnership**, a shared responsibility between you and us, between your business and technical experts, and our architects, security experts, and operations personnel. We believe that this is the only way to not only create a technical architecture that reduces the possibility of introducing vulnerabilities into your application, but also to create clarity and understanding about the processes and the proactive and reactive measures that must be put in place. More importantly, realizing that Security is a shared responsibility helps you and Rackspace focus on providing transparency on the roles and responsibilities of *each party*. From your organization to Rackspace, everybody must understand their role as part of a business relationship based on trust.

Let's now focus on how this relationship manifests itself through an example. Before we do that, we will introduce a framework that helps understand these responsibilities.

4. Rackspace's Security Vision and the PDCA cycle

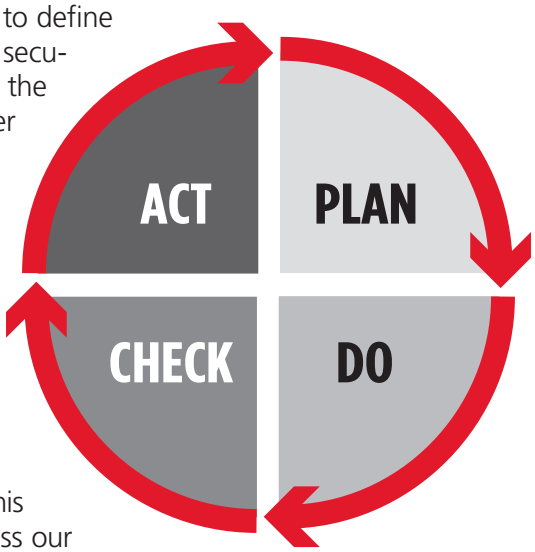
At Rackspace, our vision in Security is to deliver a Customer Security Program that combines Rackspace expertise with technology and services that results in a differentiated service level for you and your business goals, whether on dedicated infrastructure or on our public cloud, by leveraging our trusted relationship with customers like you.

By virtue of having engaged with thousands of customers over the lifetime of our company, we have developed a model based on Dr. W. Edwards Deming's Plan-Do-Check-Act management method, which is the foundation of control and process improvement for the delivery of products and services. This method, sometimes referred to as the Deming Wheel or Shewhart cycle, defines a cycle with the following four steps[1]:

1. **PLAN**
2. **DO**
3. **CHECK**
4. **ACT**

[1] Refer to this page from the American Society of Quality: http://asq.org/learn-about-quality/project-planning-tools/overview/pdca-cycle.html, which is based on Nancy R. Tague's The Quality Toolbox, Second Edition, ASQ Quality Press, 2004, pages 390-392

In the **PLAN** step of the cycle we work with you to define the goals, expectations and requirements for the security management of your environment, as well as the policies, processes and activities required to deliver on those results. In this step, we also identify the metrics and the data sources that will be needed to measure the process success. In the **DO** step, we implement the security controls based on those requirements and expectations, and work with you to help ensure we are all doing our respective tasks and fulfilling our respective roles, and collect the right data to monitor the security program for your environment. For the **CHECK** step, we monitor the security controls we have established together. This involves measuring the instrumentation data across our infrastructure and your application. We also establish proactive and reactive engagements with you to help with those parts of the infrastructure that are under your control and ensure they are also checked, and decide on whether any corrective actions must be implemented. Finally, in the **ACT** step, we implement those actions (both proactively and reactively) on our platform, and work with you to implement those actions on the elements of the infrastructure under your control.



5. Security Management and the PDCA Cycle

It is not the goal of this white paper to cover all the technical disciplines involved in securing your infrastructure or applications, or to discuss in detail Rackspace's security policies for buildings, personnel and data centers. However, it may be valuable to discuss how certain security disciplines align with the PDCA cycle.

Let's use the example of a PCI initiative. PCI (as the Payment Card Industry Data Security Standard is widely known) is a compliance standard that establishes a set of controls for organizations that are involved in processing credit card payments and other payment-related sensitive data. Its goal is to prevent the misuse of cardholder information[2]. Let's discuss now each step in the PDCA cycle:

- **PLAN**: Typically, the PLAN step would be a conversation that, while supported by the challenges of the technology and its reality, tries to focus on the goals and expectations of your initiative. No single approach is applicable to every situation. Many customers have well-defined requirements for which Rackspace solutions are a good fit, while others prefer Rackspace Professional Services which can help drive the planning, assessment and recommendations on appropriate solutions to help with specific security and compliance requirements.
- **DO**: In the DO step, we focus on specific PCI controls. For example, we implement SSL Certificates to address the PCI requirement about the encrypted transmission of cardholder data across open, public networks; or we may implement solutions such as Managed Active Directory to help address the PCI requirement of restricting access to cardholder data by business need-to-know.
- **CHECK**: In the CHECK step, we monitor the resources of the infrastructure, and respond to changes in the security infrastructure. We incorporate services such as Penetration Testing, Threat Management, and Log Management, to name some. More importantly, we use the Vulnerability Assessment reports from your infrastructure not just as a "checkbox" to make our customers "feel good," but to drive meaningful conversations about other actions that may be required.
- **ACT**: Finally, we ACT together. We implement the necessary changes by coordinating work across your IT security and systems personnel, developers and architects, with Rackspace's systems engineers, architects, and support personnel, all of whom are dedicated to the delivery of Fanatical Support. It is the dedication of these Rackers that generate comments like the one above.

> *"It is probably true to say that without the considerable amount of help from Rackspace we could not have passed the exceptionally stringent PCI audit. Rackspace certainly went above and beyond their remit to ensure that everything was perfect for us."*
>
> – Aingaran Somaskandarajah, Technical Lead, Oyster Card

[2] For more detailed information about Rackspace's PCI, please refer to http://www.rackspace.com/ecommerce-hosting/pci/

6. Conclusion

The sophistication level of the next generation of cloud-based applications is increasing, and with it, the security landscape is turning more complex. The consequences of inaction can negatively impact your ability to do business. Pay attention to the details of the relationship as you consider any hosting or cloud provider (including Rackspace). Get personally involved and have your technical personnel drive meaningful relationships with the experts of your cloud provider. These relationships can go a long way towards creating the atmosphere of trust and support required for a successful initiative. At Rackspace, our employees provide Fanatical Support across the lifecycle of your service, from planning to retirement, and building this relationship is part of how we do business. But even if Rackspace is not your cloud provider, still recognize that Security is a Partnership, a shared responsibility. Build a relationship with your cloud provider and make sure they participate in it. More importantly, get into the details of the technology, processes and policies to ensure that an appropriate security level. Remember that you must do your part in helping secure your infrastructure and applications.

DISCLAIMER

This whitepaper is for informational purposes only and is provided "AS IS." The information is intended as a guide and not as a step-by-step process, and does not represent an assessment of any specific compliance with laws or regulations or constitute advice. We strongly recommend that you engage additional expertise in order to further evaluate applicable requirements for your specific environment.

RACKSPACE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS DOCUMENT AND RESERVES THE RIGHT TO MAKE CHANGES TO SPECIFICATIONS AND PRODUCT/SERVICES DESCRIPTION AT ANY TIME WITHOUT NOTICE. RACKSPACE RESERVES THE RIGHT TO DISCONTINUE OR MAKE CHANGES TO ITS SERVICES OFFERINGS AT ANY TIME WITHOUT NOTICE. USERS MUST TAKE FULL RESPONSIBILITY FOR APPLICATION OF ANY SERVICES AND/OR PROCESSES MENTIONED HEREIN. EXCEPT AS SET FORTH IN RACKSPACE GENERAL TERMS AND CONDITIONS, CLOUD TERMS OF SERVICE AND/OR OTHER AGREEMENT YOU SIGN WITH RACKSPACE, RACKSPACE ASSUMES NO LIABILITY WHATSOEVER, AND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO ITS SERVICES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

Except as expressly provided in any written license agreement from Rackspace, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property.

Rackspace, Fanatical Support, and/or other Rackspace marks mentioned in this document are either registered service marks or service marks of Rackspace US, Inc. in the United States and/or other countries.

Third-party trademarks and tradenames appearing in this document are the property of their respective owners. aSuch third-party trademarks have been printed in caps or initial caps and are used for referential purposes only. We do not intend our use or display of other companies' tradenames, trademarks, or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.