CHAPTER

8

Useful Next Steps and Approaches

Removing the faults in a stage-coach may produce a perfect stage-coach, but it is unlikely to produce the first motor car.

—Edward de Bono

With the large volume of information on cloud computing and security presented in the previous chapters, it is valuable to use that information to make important decisions and find answers to common questions concerning the application of cloud computing in an organization.

This chapter focuses on exploring the questions to ask cloud providers when considering their services, the categories of applications that should be placed on the cloud, the type of cloud to be used, areas to obtain additional cloud information and assistance, and how to get started in cloud computing.

Getting Answers

Three common questions come up when an organization is considering using a cloud:

- What services should I move to the cloud?
- What questions should I ask the cloud provider?
- When should I use a public, private, or hybrid cloud?

These questions are addressed in the following sections.

What Services Should Be Moved to the Cloud?

One of the most important considerations in deciding which services should be placed on a cloud is cost. Cloud expenses include charges for storage, processing time, and bandwidth consumption. Bandwidth costs can be extremely high; therefore, a cloud application that involves a large amount of data being exchanged with a cloud over extended periods of time would not be a good cloud candidate. Also, applications that have a high degree of parallelism can be run more efficiently on cloud systems using available distributed processing frameworks such as Map/Reduce and Hadoop.

Another important consideration, especially for companies involved in e-commerce, is availability and resilience. Critical applications that can affect an organization's mission should not be placed on the cloud, and the cloud provider should demonstrate that its system exhibits resiliency in the event of system crashes and unexpected events.

Applications should be designed such that they can be moved from one cloud provider to another, in order to avoid being locked in to a particular vendor. In addition, some laws and regulations require that critical data be kept on the organization's site and under its control.

Cloud computing can also be used to provide cost-effective backup services and to handle overflow tasks during periods of peak activity such as seasonal work.

BACKUP SERVICES

A cloud can deliver protections against disasters by providing online data backup at an alternate location. This approach avoids large investments in redundant hardware and software and enables a cloud user to recover rapidly from a harmful event. Cloud computing provides this business continuity and disaster recovery through the use of dynamically scalable and virtualized resources.

The following additional points are useful in evaluating whether or not an application is a good candidate for cloud deployment:

- If an application has speed and response-time requirements, it is probably not practical to place it on a cloud.
- If a cloud provider requires an application to be written in a certain language and has restrictions such as no VPNs, it might not be cost effective to rewrite applications and make other related changes in order to migrate to a cloud.
- Some regulations such as HIPAA require that sensitive data be managed and controlled in-house.

- If gearing up internally to develop a product or service is going to take many months, and time to market is a consideration, moving applications to a cloud might be an effective solution.
- If an application can run more effectively on a parallelized system or in a virtualized environment, then it is a good candidate for migration to the cloud.
- If an application incorporates multi-tenancy, it is a good candidate for the cloud.
- Very critical applications and highly sensitive data that are essential to the survival of an organization are better kept in-house.
- In general, if an entire process is currently being run well in-house and there are no compelling maintenance, staffing, and other resource issues, there is no need to partition it out to a cloud.
- Selected applications that involve serious liability issues might be better kept inside an organization's IT system.

What Questions Should You Ask Your Cloud Provider?

There are numerous questions that can be asked of a cloud provider, including concerns about security, performance, cost, control, availability, resiliency, and vendor lock-in. Some of the critical questions that should be asked that address these concerns are as follows:

- Do I have any control or choice over where my information will be stored? Where will my data reside and what are the security and privacy laws in effect in those locations?
- Are your cloud operations available for physical inspection?
- Can you provide an estimate of historical downtimes at your operation?
- Are there any exit charges or penalties for migrating from your cloud to another vendor's cloud operation? Do you delete all my data from your systems if I move to another vendor? How do you prove to me that you have completely removed all my data from your cloud system?
- Can you provide documentation about your disaster recovery policies and procedures and how they are implemented?
- What are your organization's privacy policies and policies addressing ownership of client data?
- Will you provide a sample of your log files so that the types of data being recorded are available for review?

- What are your policies concerning my sensitive information when a law enforcement agency presents a subpoena for that data? What protections for my information can you provide in this event?
- Will you provide samples of your SLA?

If an application involves real-time streaming media, it is important to ask the cloud provider if its load-balancing approach supports *direct server return (DSR)*. In DSR, server data is sent directly to the client without having to go through intermediate, delay-inducing processing, such as a load balancer.

An obvious question is "How can the client determine if an instance of an application is available and if multiple instances have been unnecessarily launched?" Superfluous instances can result in higher costs; and, conversely, a client should have the assurance that an instance will be relaunched after a system failure.

It is also important to determine the cloud provider's auditing practices and liability protections, as well as authentication, authorization, and other security processes. For example, does the vendor encrypt the client's data both in storage and during transmission? What types of encryption technologies are employed? Are employees vetted to ensure they will not compromise critical data on the cloud?

The user has to understand how the cloud provider implements the provisioning and de-provisioning of resources and if these functions can be accomplished on demand and in an automated fashion. The provider should also be asked to explain its fail-over policies and capabilities.

While there are probably many more areas that have to be examined, the answers to these questions and concerns will give a potential cloud user a fairly good picture of the cloud provider's capabilities, responsibilities, and approaches to protecting client data.

When Should You Use a Public, Private, or Hybrid Cloud?

Recall that a private cloud is owned and controlled by a single party whose services are provided on a private network. The hardware and software are purchased by the private organization; and it may be housed on or off the organization's premises, and could be managed by the organization or a third party. Following are the principal advantages of using a private cloud:

- Delivery of cloud economic and flexibility benefits inside an organization
- Means to develop and debug new applications and then eventually transfer them to a public cloud
- Means to meet regulatory and legal requirements without having to interact with a cloud provider

- Path to leveraging existing investments in computational resources, such as virtualization software
- Utilization of other available resources in proximity to the private cloud
- Ability to directly control security, sensitive applications, and data
- Capability to develop and implement desired privacy policies
- Means to control hardware characteristics and provisioning
- Ability to reduce operational costs and increase server utilization
- Opportunity to increase use of automation and standards

A public cloud, which provides a shared computing environment through the Internet, is more efficient because of common resources, but it poses more security risks. A public cloud is a good choice if the following conditions exist:

- Budget limitations on capital expenditures for computing resources.
- Application code has to be developed and tested.
- Preference for a pay-as-you-go model.
- Desire to reduce IT operational and maintenance staff.
- Additional computing resources are needed on an intermittent basis, such as for seasonal workloads.
- Availability of large Internet bandwidth.
- It's necessary to support a large number of collaborative projects.
- SaaS applications can be provided by a trusted vendor.
- Applications are widely used and better implemented off-site, such as e-mail.

In general, a private cloud provides control and a more secure environment for sensitive applications and data, while a public cloud is more cost effective and provides increased flexibility and scalability. The confluence of these characteristics leads to consideration of a hybrid cloud, which is a combination of a public and private cloud. A hybrid cloud involves multiple providers and a plurality of platforms to manage and protect. A hybrid cloud is useful in the following situations:

- An organization uses a public cloud to communicate and exchange information with clients and partners, but protects associated data on an internal, private cloud.
- An organization has policies and means in place to manage and control movement of work projects in and out of the cloud.

- An organization has the ability to make decisions about where to run applications depending on changes in cost structures and services.
- An organization has the means and policies in place to ensure that regulatory and legal requirements are met when moving applications between private and public cloud environments.
- An organization needs secure SaaS applications and uses a private cloud provided by a cloud vendor.

Getting Help

Several working groups and forums have been established both to support the exchange of information among cloud users and potential users and to advance the development of cloud computing standards. These organizations welcome new participants and encourage discussions on topics of interest to the cloud community. A few of the prominent groups are summarized in the following sections.

Cloud Security Alliance

The stated mission of the Cloud Security Alliance (`http://www.cloudsecurity-alliance.org/`) is "to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing." The Alliance has published a document titled "Security Guidance for Critical Areas of Focus in Cloud Computing," which can be viewed at `http://www.cloudsecurity-alliance.org/guidance/csaguide.pdf`. The document defines the following 15 domains that are critical in cloud security:

- Cloud Architecture
  - Domain 1: Cloud Computing Architectural Framework
- Governing in the Cloud
  - Domain 2: Governance and Enterprise Risk Management
  - Domain 3: Legal
  - Domain 4: Electronic Discovery
  - Domain 5: Compliance and Audit
  - Domain 6: Information Lifecycle Management
  - Domain 7: Portability and Interoperability

- Operating in the Cloud
  - Domain 8: Traditional Security, Business Continuity and Disaster Recovery
  - Domain 9: Data Center Operations
  - Domain 10: Incident Response, Notification and Remediation
  - Domain 11: Application Security
  - Domain 12: Encryption and Key Management
  - Domain 13: Identity and Access Management
  - Domain 14: Storage
  - Domain 15: Virtualization

Interested parties can obtain a complimentary membership in the Alliance through their LinkedIn location at `http://www.linkedin.com/groups?gid=1864210`. Current members include HP, AT&T, Dell, MacAfee, and Microsoft.

In addition, industry groups and not-for-profit groups can become affiliates of the Cloud Security Alliance. Information on the affiliates program is available at `affiliates@cloudsecurityalliance.`

Cloud Computing Google Groups

Google Groups provides the means for individuals and organizations to set up a Group site devoted to a special interest or topic. Having done so, group members can communicate through the Web or e-mail to exchange information on their subjects of interest.

The Cloud Computing Google Group website is located at `http://groups.google.com/group/cloud-computing`. Google Group rules allow the following interactions with the website:

- Anybody can view group content.
- Only managers can view a group's members list.
- People can request an invitation to join.
- Members can create and edit pages.
- Only managers can upload files.
- Only members can post.
- All messages are held for moderation.
- Messages from new members are moderated.

Anyone wishing to join the Cloud Computing Google Group can apply at http://www.linkedin.com/e/gis/61513/6213F13BB1AA.

Cloud Computing Interoperability Forum

The Cloud Computing Interoperability Forum (CCIF) (http://www.cloudforum.org) defines its mission as follows: "CCIF is an open, vendor neutral, open community of technology advocates, and consumers dedicated to driving the rapid adoption of global cloud computing services. CCIF shall accomplish this by working through the use of open forums (physical and virtual) focused on building community consensus, exploring emerging trends, and advocating best practices/reference architectures for the purposes of standardized cloud computing."

CCIF members include Intel, Cisco, Sun, IBM, and RSA.

The motivation for the CCIF was to define a common cloud computing interface and uniform definitions to support interoperability among cloud vendors.

The CCIF conducts meetings and workshops to involve the broad cloud computing community in the determination of appropriate standards and best practices and to develop vendor-neutral approaches.

Open Cloud Consortium

The Open Cloud Consortium (OCC) (opencloudconsortium.org/) comprises universities and vendors, and is focused on standards and open frameworks to promote cloud interoperability. OCC members include Cisco, Northwestern University, Johns Hopkins University, the University of Chicago, and the California Institute for Telecommunications and Information Technology (Calit2). The stated goals of the OCC are as follows:

- Manage and operate an open cloud testbed.
- Generate cloud computing benchmarks.
- Develop cloud computing standards and frameworks to promote interoperability.
- Conduct workshops relating to cloud computing.

The Open Cloud Consortium is organized into the following four working groups:

- **Working Group on Standards and Interoperability for Large Data Clouds —** Develops standards for interoperability among large data clouds such as Hadoop Map/Reduce and distributed file systems. Hadoop Map/Reduce is a software framework for developing applications

that parallel process terabytes of data on large numbers of computing nodes.

- **The Open Cloud Testbed Working Group** — Operates the Open Cloud Testbed. Membership is restricted to participants that can contribute resources to the testbed.
- **The Open Science Data Cloud (OSDC) Working Group** — Operates a large data cloud to support research. Members of this group include the Institute for Genomics and Systems Biology at the University of Chicago, Johns Hopkins University, the Laboratory for Advanced Computing at the University of Illinois at Chicago, and Northwestern University.
- **Intercloud Testbed Working Group** — Operates a testbed to explore the services of the Interface to Metadata Access Point (IF-MAP) protocol. IF-MAP supports integrated security by providing the capability for security mechanisms such as intrusion detection systems to acquire and share information that can be evaluated by MAP for security breaches.

Membership information for the consortium can be found at `http://opencloudconsortium.org/membership-documents/`.

Getting Started

Fortunately, it's easy to get started in cloud computing; unfortunately, it's a problem if your IT department isn't prepared. Remember that just because this technology now has the word "cloud" in front of it, it doesn't mean that traditional information systems security standards don't apply.

This is especially important when an organization begins to shift to virtual all-cloud operations. Now the lion's share of your computing systems may move under the control of a third-party provider. Your task is to not only acquire cloud services that can fit with your internal systems, but also guarantee that the new cloud services interoperate with your traditional infrastructure.

Cloud computing can make it difficult for security professionals to implement best practices, both in-house and when using Cloud Service Providers (CSPs). In this section, we'll take a high view, and give you some pointers on the best way to start your cloud computing security journey.

Top Ten List

We've given you a ton of information and advice throughout the book, so here we'll try to condense it down to just a few points to get you started. Okay, there's more than just ten items here, but it's easier to digest if you create a hierarchical system.

1. Assess Your Data's Sensitivity

You need to know how much security is enough, and to do that you need to know the security needs of your data. Therefore, companies should assess the sensitivity of the data they are considering moving to the cloud.

There's several ways to approach this determination. You might be subject to various compliance regulations that will require data sensitivity classification, such as the following:

- BASEL II
- DoD Directive 8500.1
- FISMA
- Gramm-Leach-Bliley
- HIPAA
- NERC
- Payment Card Industry (PCI) Data Security Standard
- Sarbanes-Oxley

You might decide to identify your information data assets and then institute data classification security management practices. That means classifying your organization's assets and rating their vulnerabilities so that effective security controls can be implemented.

The Information Classification Process

The information that an organization processes must be classified according to the organization's sensitivity to its loss or disclosure. The information system owner is responsible for defining the sensitivity level of the data. Classification according to a defined classification scheme enables the security controls to be properly implemented.

Implementing information classification has several clear benefits to an organization, such as:

- It demonstrates an organization's commitment to security protections.
- Classification helps identify which information is the most sensitive or vital to an organization.
- It supports the tenets of confidentiality, integrity, and availability as it pertains to data.
- It also helps identify which protections apply to which information.
- Classification might be required for regulatory, compliance, or legal reasons.

The following classification terms are often used in the private sector:

- **Public** — Information that is similar to unclassified information; all of a company's information that does not fit into any of the next categories can be considered public. While its unauthorized disclosure may be against policy, it is not expected to impact seriously or adversely the organization, its employees, and/or its customers.
- **Sensitive** — Information that requires a higher level of classification than public data. This information is protected from a loss of confidentiality as well as from a loss of integrity due to an unauthorized alteration. This classification applies to information that requires special precautions to ensure the integrity of the information by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness.
- **Private** — This classification applies to personal information that is intended for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees. For example, salary levels and medical information are considered private.
- **Confidential** — This classification applies to the most sensitive business information that is intended strictly for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners, and/or its customers. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. For example, information about new product development, trade secrets, and merger negotiations is considered confidential.

In all of these categories, in addition to having the appropriate clearance to access the information, an individual or process must have a "need to know" the information. Thus, individuals cleared for high data classification levels may still not be authorized to access classified material at that same level if it is determined that access to that material is not needed for them to perform their assigned job functions. Table 8-1 shows a simple data classification scheme for the private sector. This is a very high level scheme, and is used to begin the classification process.

Table 8-1: Private/Commercial Sector Information Classification Scheme

DEFINITION	DESCRIPTION
Public Use	Information that is safe to disclose publicly
Internal Use Only	Information that is safe to disclose internally but not externally
Company Confidential	The most sensitive need-to-know information

Alternatively, an organization may use the high, medium, or low classification scheme based upon its data sensitivity needs and whether it requires high, medium, or low protective controls. For example, a system and its information may require a high degree of integrity and availability, yet have no need for confidentiality.

The designated owners of information are responsible for determining data classification levels, subject to executive management review. Table 8-2 shows a simple H/M/L data classification for sensitive information.

Table 8-2: H/M/L Data Classification

CATEGORY	DESCRIPTION
High	Could cause loss of life, imprisonment, major financial loss, or require legal remediation if the information is compromised
Medium	Could cause noticeable financial loss if the information is compromised
Low	Would cause only minor financial loss or require minor administrative action for correction if the information is compromised

(Source: NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems.")

Classification Criteria

Several criteria may be used to determine the classification of an information object:

- **Value** — Value is the number one commonly used criteria for classifying data in the private sector. If the information is valuable to an organization or its competitors, it needs to be classified.
- **Age** — The classification of information might be lowered if the information's value decreases over time. In the Department of Defense, for example, some classified documents are automatically declassified after a predetermined time period has passed.
- **Useful life** — If the information has been made obsolete due to new information, substantial changes in the company, or other reasons, the information can often be declassified.
- **Personal association** — If information is personally associated with specific individuals or is addressed by a privacy law, it might need to be classified. For example, investigative information that reveals informant names might need to remain classified.

Information Classification Procedures

There are several steps in establishing a classification system. These are the steps in priority order:

1. Identify the administrator and data custodian.
2. Specify the criteria for classifying and labeling the information.
3. Classify the data by its owner, who is subject to review by a supervisor.
4. Specify and document any exceptions to the classification policy.
5. Specify the controls that will be applied to each classification level.
6. Specify the termination procedures for declassifying the information or for transferring custody of the information to another entity.
7. Create an enterprise awareness program about the classification controls.

2. Analyze the Risks vs. Benefits of Cloud Computing

It's also very important to consider the risks and benefits of cloud computing. This can be done by executing a traditional risk assessment, while focusing it on the risk/benefit of exploiting the cloud.

Risk Management

Adopting a flexible risk management process can be a big help, if you don't do this already. RM is the identification, analysis, control, and minimization of loss that is associated with events. RM's main function is to mitigate risk. Mitigating risk means reducing risk until it reaches a level that is acceptable to an organization.

The risk management process minimizes the impact of threats realized and provides a foundation for effective management decision making. As defined in NIST SP 800-30, risk management is composed of three processes:

- Risk assessment
- Risk mitigation
- Evaluation and assessment

The RM task process has several elements, primarily including the following: performing a risk analysis; including the cost-benefit analysis of protections; and implementing, reviewing, and maintaining protections.

To enable this process, you need to determine some properties of the various elements, such as the value of assets, threats, and vulnerabilities, and the likelihood of events. A primary part of the RM process is assigning values to threats and estimating how often (or how likely) that threat might occur.

The identification of risk to an organization entails defining the following basic elements:

- The actual threat
- The possible consequences of the realized threat
- The probable frequency of the occurrence of a threat
- Confidence level that the threat will happen

Many formulas and processes are designed to help provide some certainty when answering these questions. Of course, because these threats are constantly evolving, it is impossible to consider every possibility. Risk management is an attempt to anticipate, to the extent possible, future threats, and to lower the possibility of their occurrence (and subsequent impact on the company).

It's important to remember that the risk to an enterprise can never be totally eliminated; that would entail ceasing operations. Risk management means finding out what level of risk the enterprise can safely tolerate and still continue to function effectively.

Trade-off Analysis

As you consider security management controls, a cost versus benefit analysis is a very important process. The need for, or value of, a particular security control must be weighed against its impact on resource allocation. A company can have exemplary security with a seemingly infinite budget, but there is always a point of diminishing returns, when the security demands interfere with the primary business. Making the financial case to upper management for various security controls is a very important part of a security manager's function.

A trade-off analysis can be formal or informal, depending upon the audience and the intent of the analysis. If the audience of the TOA is higher management or a client, often a formalized TOA, supported by objective evidence, documentation, and reports, will be necessary. If the TOA will be examined by internal staff or departments, often it can be less formal; but the fundamental concepts and principles still apply in either case.

Cloud Cube Model

The Jericho Forum's Cloud Cube model we described in Chapter 4 is a good starting point for determining the value of a cloud-based technology; it can help you get a better handle on the security issues associated with a specific flavor of cloud.

The Cloud Cube models suggests you ask four fundamental questions about your proposed cloud implementation:

- Is it an internal or external cloud?
- Does it use proprietary or open technology?

- Is the cloud service outsourced or done in-house?
- Does the cloud work within the company's security perimeter, such as a network firewall, or outside it?

Answering these four questions will help you to determine the necessary security controls.

3. Define Business Objectives

Early in the requirements process, approach cloud security from a higher level in the organization. That is, initially define business objectives, not technical objectives. Consider the following four aspects of any business objectives:

- **Business** — What are the vendor integration challenges? How important is data portability? Which data should remain in house?
- **Financial** — Build it or buy it? What are the costs of data loss? What should be part of a disaster recovery plan?
- **Legal and regulatory** — Key regulations include HIPAA and state data protection laws.
- **Technical** — These issues include authentication, data integrity, data flow, and privacy assessment.

4. Understand the Underlying Structure of Your Network

By creating application and network diagrams of the security architecture, you will understand the underlying cloud structure better and be better able to reach your security control objectives.

The network diagram should cover how the data travels through your network (data in motion), where it's stored (data at rest), and who's using it and how (data in use). You'll also need to know how cloud vendors are interacting with your applications, as this will affect security concerns.

INSTITUTE A LAYERED SECURITY ARCHITECTURE

In order to create a sound security architecture, consider a layered approach to addressing threats or reducing vulnerabilities. For example, using a packet-filtering router in conjunction with an application gateway and an intrusion detection system increases the amount of effort an attacker must expend to successfully attack your system.

5. Implement Traditional Best Practice Security Solutions

To preserve security of your private cloud-based virtual infrastructure, enact security best practices at both the traditional IT and virtual cloud layers. Traditional computer security best practices that translate directly to virtual environments include the following:

- **Encryption** — Use encryption wisely and make it well-focused. The sensitivity of the data may require that the network traffic to and from the VM be encrypted, and full disk encryption might also be required, using encryption at the host OS or hypervisor level. However, encryption isn't a panacea for a poorly designed security architecture; use it sparingly and examine your options for file encryption, volume encryption, and disk encryption carefully.
- **Physical security** — Sometimes the most obvious risk is the most serious and often overlooked. Keep the virtual system (and cloud management hosts) safe and secure behind carded doors, and environmentally safe.
- **Authentication and access control** — Authentication and access control lie at the foundation of a successful security program. The authentication capabilities within your virtual system should mimic the way your other physical systems authenticate. Two-factor authentication, one-time passwords, and biometrics should all be implemented in the same manner.
- **Separation of duties** — As systems get more complex, misconfiguration is more likely. Lack of expertise coupled with insufficient communication can make this more likely. Be sure to enforce least privileges with access controls and accountability.
- **Configuration, change control, and patch management** — This is very important, and sometimes overlooked in smaller organizations. Configuration and change control, patch management, and update processes need to be maintained in the virtual world as well as the physical world.
- **Intrusion detection and prevention** — As mentioned in Chapter 5, know what's coming into and going out of your network. A host-based intrusion prevention system coupled with a hypervisor-based solution could examine both virtual network traffic and traffic to the box.

6. Employ Virtualization Best Practices

A virtualized system also requires its own set of best practices, above and beyond the traditional physical IT security best practices (BPs) already described. Remember that these best security practices involve both processes and

technologies; don't get so caught up in a shiny, magic bullet that you overlook processes and procedures. These best practices include the following:

- Enforce least privileges.
- Harden access controls.
- Monitor virtual traffic.
- Don't combine in-scope and out-of-scope VMs.
- Implement one primary function per VM.
- Track VM migrations.
- Include offline VMs in the patching process.
- Decommission VMs when they are no longer needed.
- Implement VM life cycle management.
- Bind sensitive VMs to separate physical network interfaces.
- Monitor VM snapshots and rollback.
- Scan and audit VMs prior to deployment.

7. Prevent Data Loss with Backups

Always backup, backup, and backup again. Computers fail, so plan for failure through redundancy and backups. Some cloud vendors provide backup services or data export processes, enabling companies to create their own backups. Other cloud vendors require you to use a custom solution or provide your own third-party application.

In addition, ensure that the backup stream traversing the cloud is encrypted, and that the physical backup location and media transfer and storage are also secure. In any event, know how your backup is being performed, and schedule regular restore tests. Be sure you know how to access the cloud vendor for the restore procedure if you've suffered a catastrophic failure.

8. Monitor and Audit

Monitor continually and audit frequently. Your cloud vendor must be able to guarantee that it can monitor who has accessed your data. Even though you may not control vulnerability monitoring in a public cloud scenario, you're still accountable for risk to the enterprise. Therefore, you'll need to assess the efficacy of the vendor's auditing program. Cloud vendors are going to be improving in this area, as each vendor seeks to be differentiated from the pack.

9. Seek Out Advice

Sometime a little knowledge can be a dangerous thing. Fortunately, a wealth of information is beginning to be disseminated about cloud security. In addition, the following three main resources are useful in securing your virtual infrastructure:

- **Cloud Security Alliance (CSA)** — We've described them before, and can't mention them enough. The CSA published its first security guideline in April 2009: "Security Guidance for Areas of Focus in Cloud Computing." There is now a Version 2.1 (`www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf`) that continues its mission to "create and apply best practices to secure cloud computing." The CSA recognizes that a secure cloud is a "shared responsibility," and as such, the guidance it provides applies to both users and providers.
- **European Network and Information Security Agency (ENISA)** — In November 2009, the European Network and Information Security Agency (ENISA) brought together more than two dozen contributors to prepare and publish its "Cloud Computing: Benefits, Risks and Recommendations for Information Security." The contents of the ENISA cloud computing guide include detailed discussions on the benefits, risks, and vulnerabilities of cloud computing
- **National Institute of Science and Technology (NIST)** — NIST is the granddaddy of computer security documents, and has recently begun creating guidelines for secure cloud computing (`http://csrc.nist.gov/groups/SNS/cloud-computing`). Expect much more from this organization soon.

CLOUD DATA MANAGEMENT INTERFACE (CDMI)

The Storage Networking Industry Association (SNIA) (`http://cdmi.snia-cloud.com`) has generated the open Cloud Data Management Interface (CDMI) standard, version 1.0. The CDMI is designed to manage access to and storage of data on the cloud, and is based on the model of on-demand delivery of virtualized storage. This standard is important because it supports interoperability of the cloud storage mechanism among different cloud service providers.

The CDMI standard builds on the existing functional and management cloud interfaces and offers an interface model that can be used as the basis for future cloud storage interfaces.

As stated in the standard document, "the SNIA Cloud Data Management Interface (CDMI) is the functional interface that applications may use to create, retrieve, update, and delete data elements from the cloud. As part of this interface, the client will be able to discover the capabilities of the cloud storage offering and to use this interface to manage containers and the data that is placed in them."[1]

An important characteristic of this interface is that it can be used in a complementary fashion with existing propriety interfaces. The CDMI specification employs Representational State Transfer (RESTful) principles in its design. These principles embody features similar to those of the World Wide Web, whereby clients and servers interact and transfer data among each other. The RESTful principles were developed by Roy Fielding and described in the context of HTTP in his doctoral dissertation (see `http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm`). CDMI employs a variety of security mechanisms, including encryption, authorization, access controls, transport security, and media sanitization.

10. Employ Deception

A *honeypot* is a networked environment created solely for the purpose of identifying hackers and their activity. Usually, honeypots are impractical in the traditional IT world because of their expense, and therefore aren't employed routinely. If you aren't familiar with the concept of honeypots, we'd recommend reading the very entertaining 1989 book written by Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*.

A virtual machine honeypot, however, can be quickly set up and torn down in the DMZ, therefore reducing ownership costs. Also, the traffic can be isolated from the rest of the network, and heavy-duty IDS and monitoring can be employed.

Parting Words

Secure cloud delivery lives in a changing, challenging world, but the following benefits of virtualization can easily outweigh the risks:

- Major savings in initial capital outlay
- Important power savings, particularly now when electricity is expensive and lines are limited
- More efficient use of space in the data center
- Easier workload balancing through dynamic provisioning
- Faster deployment, rollback, and decommissioning of server farms
- Faster disaster recovery by mounting a snapshot image

We hope that this book, in addition to clearing up any cloud concerns you may have had, has given you some great new ideas and the confidence to jump into the cloud!

Notes

1. SNIA Cloud Storage Technical Working Group, `http://cdmi.sniacloud.com/`