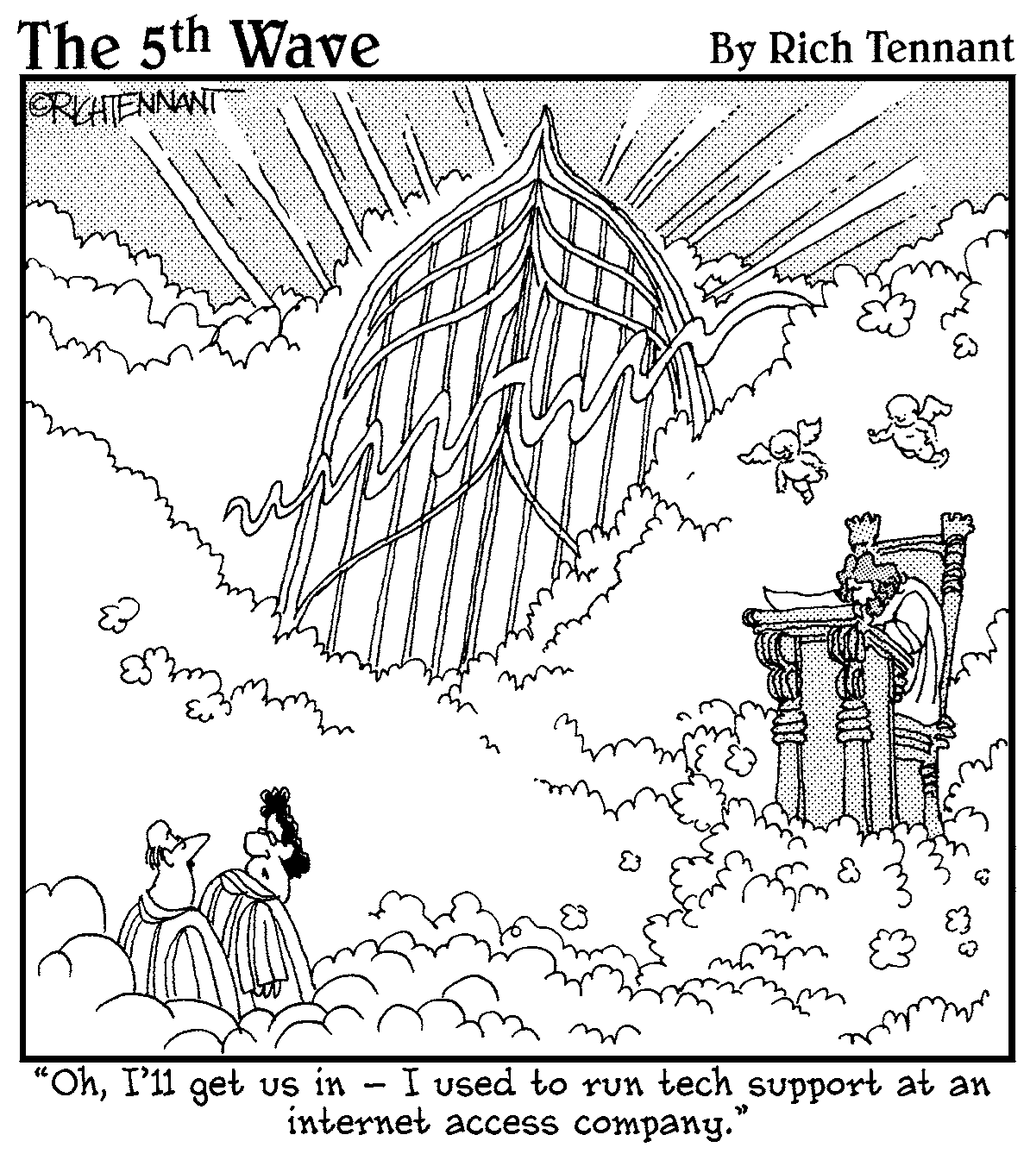
Here’s who we think you are:

✓ **You’re smart.** You’re no dummy, yet the topic of service oriented architecture gives you an uneasy feeling; you can’t quite get your head around it, and if you’re pressed for a definition, you might try to change the subject.

✓ **You’re a businessperson who wants little or nothing to do with technology,** but you live in the 21st century and find that you can’t escape it. Everybody’s saying, “It’s all about moving to the cloud,” so you think that you better find out what they’re talking about.

✓ **You’re an IT person who knows a heck of a lot about technology,** but who is new to this cloud stuff. Everybody says it’s something different. Once and for all, you want the whole picture.

Whoever you are, welcome. We’re here to help.



While there are a lot of technical considerations, keep in mind the fundamental truth: Cloud computing is a business and economic model. Is cloud computing a replacement for the traditional data center? The answer is complicated. In some cases, yes; in some cases, no.

Many players make up the world of cloud computing:

✓  The **vendors** providing applications and enabling technology, infrastructure, hardware, and integration

✓  The **partners** of these vendors that are creating cloud services offerings and providing support services to customers

✓  The **business leaders** themselves who are either using or evaluating various types of cloud computing offerings

The world of the cloud has lots of participants:

✓ The **end user** doesn’t really have to know anything about the underlying technology. In small businesses, for example, the cloud provider becomes the de facto data center. In larger organizations, the IT organization oversees the inner workings of both internal resources and external cloud resources.

✓ **Business management** needs to take responsibility for overall governance of data or services living in a cloud. Cloud service providers must provide a predictable and guaranteed service level and security to all their constituents.

✓ The **cloud service provider** is responsible for IT assets and maintenance.

Overall, the cloud embodies the following four basic characteristics:

✓ Elasticity and the ability to scale up and down

✓ Self-service provisioning and automatic deprovisioning

✓ Application programming interfaces (APIs)

✓ Billing and metering of service usage in a pay-as-you-go model

Supporting business agility

One of the most immediate benefits of cloud-based infrastructure services is the ability to add new infrastructure capacity quickly and at lower costs. Therefore, cloud services allow the business to gain IT resources in a self- service manager, thus saving time and money. By being able to move more quickly, the business can adapt to changes in the market without complex procurement processes.

A typical cloud service provider has *economies of scale* (cost advantages resulting in the ability to spread fixed costs over more customers) that the typical corporation lacks. As mentioned earlier, the cloud’s self-service capability means it’s easier for IT to add more *compute cycles* (more CPU resources added on an incremental basis) or storage to meet an immediate or intermittent needs.

With the advent of the cloud, an organization can try out a new application or develop a new application without first investing in hardware, software, and networking.

Reducing capital expenditures

You might want to add a new business application, but lack the money. You might need to increase the amount of storage for various departments. Cloud service providers offer this type of capability at a prorated basis. A cloud service vendor might rent storage on a per-gigabyte basis.

Companies are often challenged to increase the functionality of IT while minimizing capital expenditures. By purchasing just the right amount of IT resources on demand the organization can avoid purchasing unnecessary equipment. There are always trade-offs in any business situation.

A company may significantly reduce expenses by moving to the cloud and then may find that its operating expenses increase more than predicted. In other situations, the company may already have purchased significant IT resources and it may be more economically efficient to use them to create a private cloud. Some companies actually view IT as their primary business and therefore will view IT as a revenue source. These companies will want to invest in their own resources to protect their business value.

Economies of scale

The companies that provide massively scaled Software as a Service achieve *dramatic economies of scale* — cost efficiencies gained from reducing per-unit costs when more of the same item is produced or more of the same work- loads are processed.

It’s worth listing all the reasons why:

✓  The standardized workloads can be executed on a highly integrated, massively replicable infrastructure stack. They don’t have to support a wide array of workloads and a heterogeneous stack of hardware, middle- ware, OS, and so on.

✓  The computer hardware and network is highly streamlined and can be bought in bulk and configured to allow expansion. Often these companies require that hardware be engineered for their unique scaling requirements.

✓  All software can be stripped down so that only what is necessary is loaded.

✓  The service/software itself is written from scratch in a cloud-optimized way, tailored for efficiency at an instruction level.

✓  The provider may not offer or guarantee a specific service level.

✓  There is no need for virtualization technology to build virtual machines.  The software can be engineered to the bare metal.

✓  The profile of the workload is measurable and predictable simply by numbers of users.

**Internal Audit Points**

✓ How well does each cloud service perform?

✓ How are they performing together to support the business?

✓ Are the cloud services vendors adhering to governance rules that the company is required to follow?

Don’t take a supplier’s word that everything is working well. Although your company can save money in the data centers and on software licenses, you need to *spend* money and resources on service management to protect your business assets.

Cloud services impact your organization in subtle ways. The cloud impacts the whole company, not just the IT department:

✓  How do cloud services fit into your overall corporate and IT strategy? How will you manage cloud service providers along with your internal services? How will you make sure that your customers are well sup- ported by services that are moving to a cloud?

✓  Does the cloud support your corporate and IT governance requirements?

✓  What are the important issues of emerging corporate and governmental standards, business process management, and the overall issues of man- aging costs?

Governing internally provided services and the externally provided cloud- based services introduces new challenges for a company’s strategy:

✓  How do you manage the overall lifecycle of your IT resources, including software licensing, cost allocation, and charge backs?

✓  How to you protect the integrity of your information resources? How do you ensure that you’re complying with data privacy rules and regulations?

✓  How do you make sure that all your service providers can prove and document that they’re meeting governmental and corporate requirements?

Managing IT costs

All IT departments monitor costs, but few monitor them in terms of *asset performance* — the requirement to optimize the return on investments for both hardware and software. This is likely to change with the onset of cloud services. Unlike traditional licensing models, cloud propositions are based on rental arrangements.

You must compare two cost models:

✓  **Operating expenses** (paying per month, per user for each service)

✓  **Capital investments** (paying a purchase fee plus yearly maintenance for software that resides within your organization)

Evaluating the differences between the two cost models is a complex procedure for many companies. In some situations, the new cost models shift some responsibility away from IT to the business unit. For example, if a company’s business unit hires 20 new employees and email is managed in the cloud, the business unit needs to budget for 20 more users. IT doesn’t have to ensure that server capacity and IT staff are sufficient to support the additional users; that’s now the responsibility of the cloud services provider. However, IT departments need to carefully monitor the effectiveness of the cloud environment to support the enterprise.

Administering Cloud Services

A company has to ask itself many questions:

✓ Are the cloud services doing what we want them to do?

✓ How do we know if the performance is at the right level?

✓ How can we judge whether the data that was deleted is really gone?

Solving these problems isn’t easy. Investigating the reliability and viability of a cloud provider is one of the most complex areas faced when managing the cloud. The advent of cloud computing will be accompanied by disappointed customers and lawsuits for sure — some as a consequence of unrealistic expectations and some as a consequence of poor service.  It’s particularly important for IT departments to enable administration systems that let them monitor every dimension of the service they’re getting.

In theory, the cloud service provider can build and provide a very stable service that is less expensive than a customer can implement internally. However, there can be a serious gap between the actual service and the promises made in the provider’s sales literature.

You have to do your homework when evaluating the providers. Evaluate their experience in the market, the type of partnerships they’ve established, and their reputation in the market. You can also talk to other customers that have used their services.

Here are some of the issues to consider:

✓ What vendors are available to solve your problem?

✓ How effective are the providers in managing their own environment?

✓ Do they provide repeatable services?

✓ How do these vendors handle an outage?

✓ What’s their experience in dealing with customer issues?

In addition to finding a good partner, it’s always a good idea to have more than one provider as an alternative.

Service level agreements and monitoring

Every company that buys any service from a cloud service provider must either accept a standard service level agreement (SLA) from the provider or negotiate such an agreement. A *service level agreement* is a contract that stipulates the type of service you need from providers and what type of penalties would result from an unexpected business interruption.

No organization should commit mission-critical systems to the cloud with- out negotiating an SLA that includes significant penalties for not delivering the promised service level. Management needs to know what service level is appropriate under changing business conditions. Management can’t assume that the service provider will provide all the monitoring. Rather, the administrators must have their *own* ability to monitor service to satisfy the company’s goals for performance.

Support problems don’t disappear when applications or infrastructures move to the cloud. You have to make sure that support targets are agreed on in advance with a cloud services provider. Therefore, your company must align its internal support team that deals with internal customers with the cloud provider.

What processes are in place to resolve problems when they arise? Just con- sider the situation where some important application has a performance problem. Especially in a hybrid environment, it’s not always easy to tell if a problem resides within the cloud or outside of it. Such situations need to be prevented or at least dealt with very efficiently.

Billing and accounting

One cloud benefit is that, as a customer you can acquire just as much capability as needed. For this to work, billing and account management must be automated. Customers, therefore, need to be able to monitor what they’re using and how much it costs.

Potential problems arise if service level penalties aren’t clear and if the provider adds too many incidental charges. Customers can run up unexpected bills if they can’t accurately track usage.

Security in the cloud

Companies planning to use cloud services must be assured of tight, well- defined security services.

Many levels of security are required within a cloud environment:

✓ **Identity management:** For example, so that any application service or even hardware component can be authorized on a personal or group role basis.

✓ **Access control:** There also needs to be the right level of access control within the cloud environment to protect the security of resources.

✓ **Authorization and authentication:** There must be a mechanism so the right people can change applications and data.

A comprehensive security infrastructure must be provided at all levels and types of cloud services. Developers also need tools that allow them to secure the services they design to be delivered in the cloud. Organizations need consistent security across their own data center environments that intersect with a cloud service.

IT security

IT security is a major concern for new adopters of cloud computing. Ideally, you want the IT security in the cloud to integrate seamlessly with the IT security in your own data center.

However, the cloud service provider implements its own IT security procedures

✓  To protect customers from external threats

✓  To ensure that individual customer environments are isolated from one another

For every type of cloud service, the provider delivers a good deal of the IT security. You may need to understand how the cloud provider handles issues such as patch management and configuration management as the provider upgrades to new tools and new operating systems.  As the customer, you should

✓  Understand the IT security software and hardware (firewalls, intrusion detection systems, virtual private networks [VPNs], and secure connections) that the cloud provider has in place.

✓  Know how the cloud providers are protecting the overall computing environment.

Cloud Strategy

You need a strategy. Here, we list five key areas that should be part of your planning:

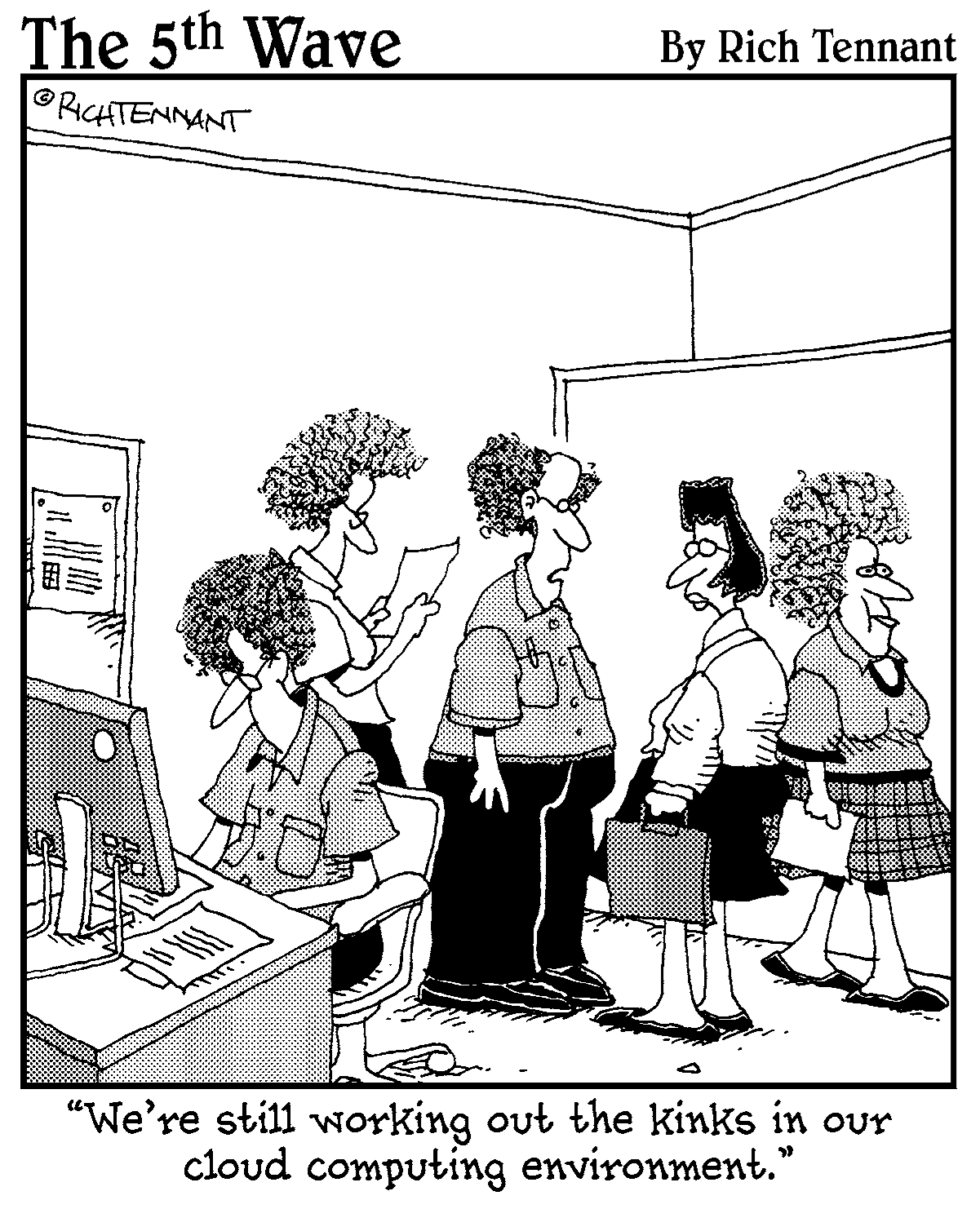
✓  When and how should you use a public, private, and hybrid cloud service?

✓  What is your company’s strategy for managing capital and operational  expenses over time?

✓  How do you plan to achieve the right level of service across the cloud and the data center?

✓  What are the rules and regulations that your cloud provider needs to adhere to, to keep your company safe and in compliance?

✓  How are you planning to control the data as it moves out of your data center into external clouds?



Costs in Clouds

We divided into four areas the places where IT spends money:

✓ **Hardware,** including servers, storage, and so on

✓ **A power supply** for those systems and how to keep them from overheating

✓ **Networking and communications equipment** so the systems can interoperate

✓ **Electricity** to support the overall data center

Examining the Economics of the Private Cloud

There isn’t one right way to evaluate the economic benefits of public or private clouds. There may be some expenses in the public cloud that only become apparent after you’re already in your project.

Before getting started, figure out which option is the most appropriate for

✓ Your company’s information technology strategy

✓ Your security strategy

✓ Your budgeting strategy

The economics of cloud computing are complicated.

Assessing capital expenditures

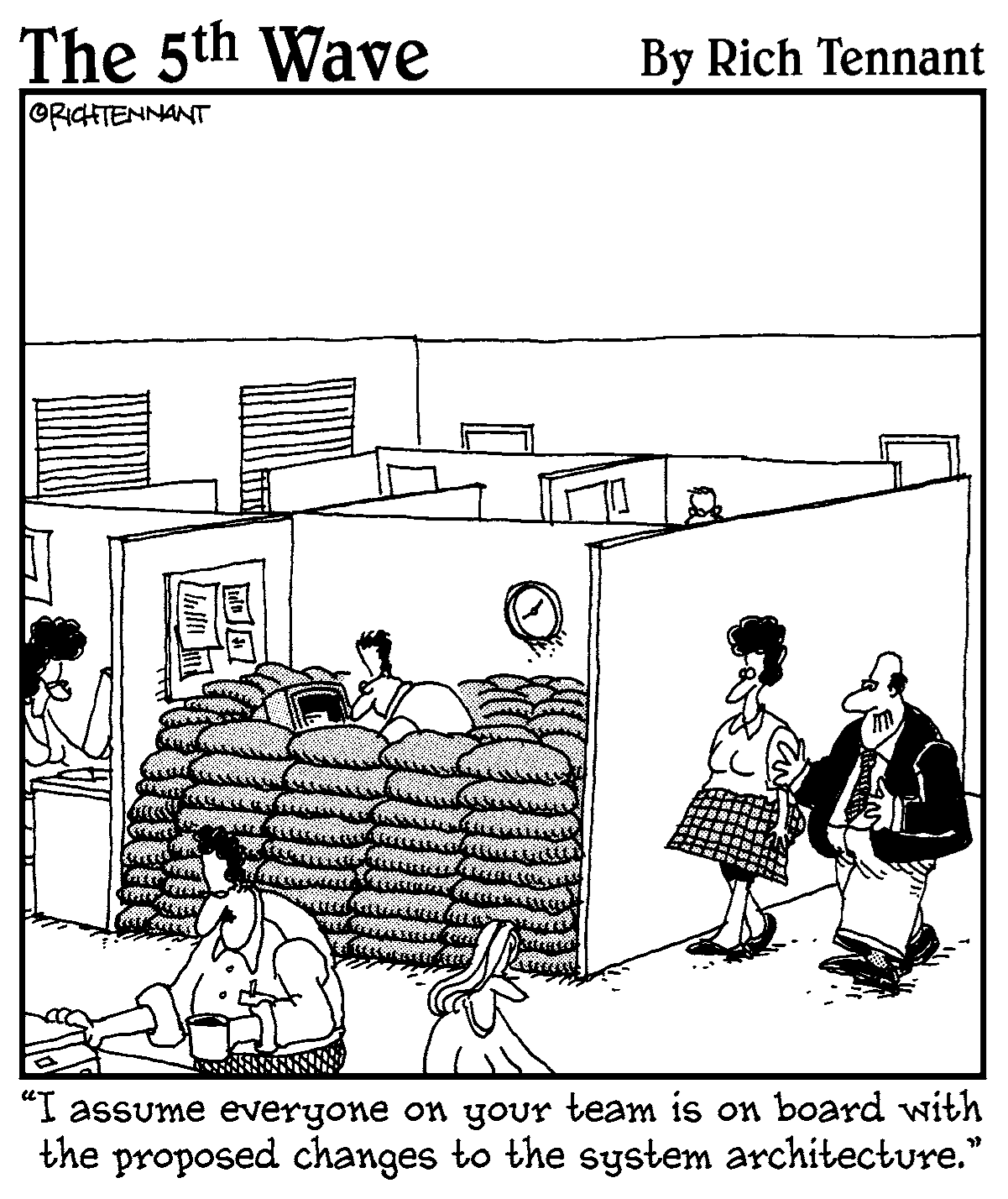
What are your data center and IT operations actually costing you? It isn’t a simple question to answer. Most companies divide the area of expenses for IT into two buckets:

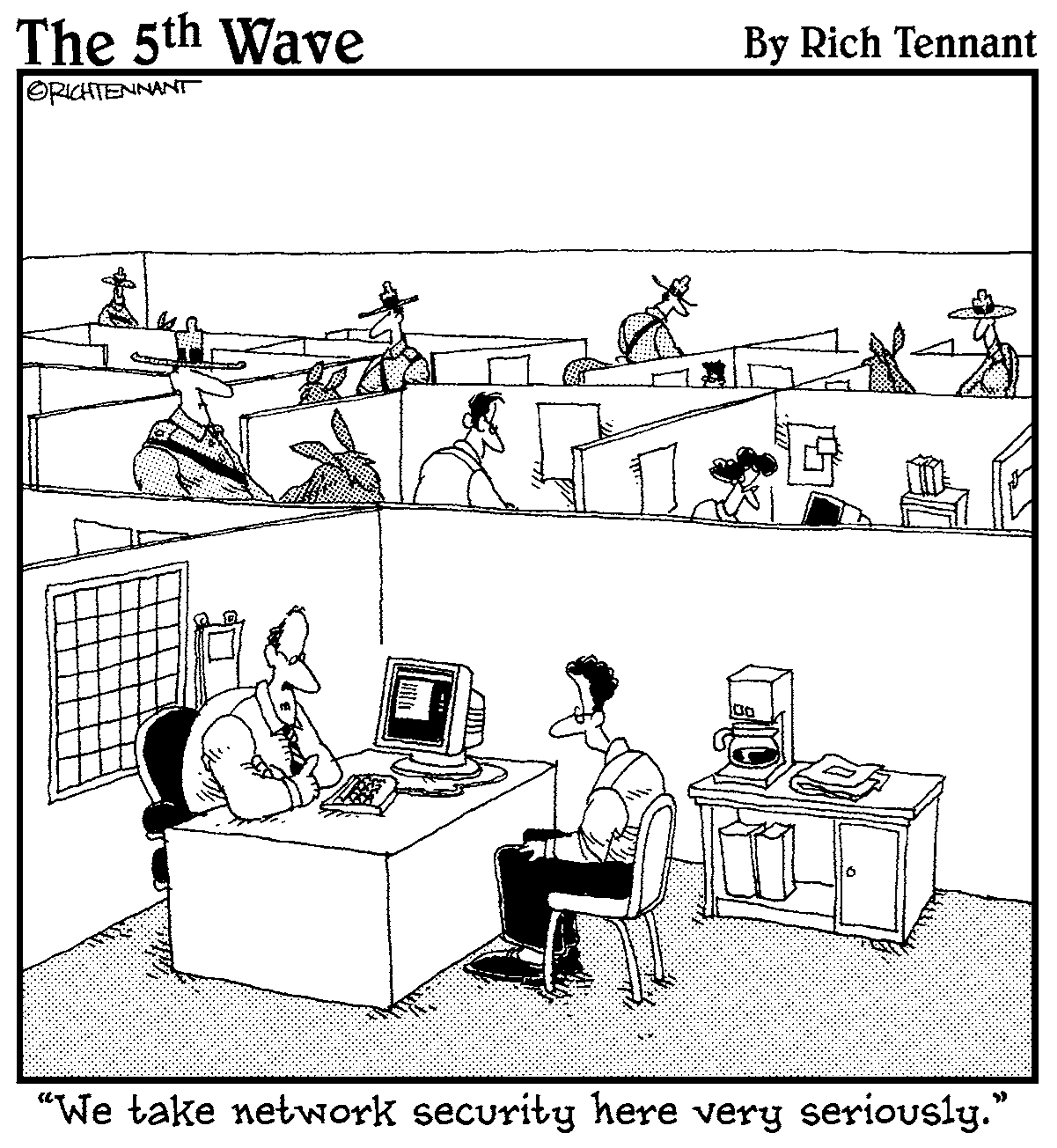
✓  Capital expenditures are spent on buying equipment (servers, networks, storage systems).

✓  Operating expenditures are the normal costs of operating a business day to day (salaries, system maintenance, and research and development).  Sometimes management likes the idea of not paying for equipment or a soft- ware package upfront. They may either want to pay in smaller, incremental payments. In this case, they might prefer a cloud platform.

✓ **Example 1:** You anticipate some big IT investment expenditures. Public cloud offerings may look economically very attractive (so you can avoid those purchases).

✓ **Example 2:** Your very large company has an excess of IT resources. You may want to work with what you have and re-architect as modular services. In addition, you might also want to add service management to support the automation of internal customers’ changing workloads.





Starting with a list of issues and questions helps you to frame the way you understand the importance of security from a cloud computing perspective.

Here are the most critical security questions to ask the potential cloud provider:

✓  What is the cloud provider’s security architecture and policy?

✓  Does the cloud provider use a third party to assess its own security risks?

✓  Does the cloud provider understand its responsibilities for governance issues (such as cross-border data transfers)?

✓  How comprehensive is the service level agreement between you and the cloud provider?

✓  Does the cloud provider understand your data preservation and protec- tion needs?

✓  Where does your data physically live? Do you have the cloud provider’s assurance that it will remain private?

✓  Does your cloud provider separate *(partition)* your data, applications, and/or management tools from other users of its cloud services?

✓  Are there clear penalties for a data or system breach?

✓  Is data portability part of the service provided by the cloud vendor?

✓  Does the cloud provider have a security baseline that it promises to adhere to?

✓  Are you allowed to inspect the cloud facility?

✓  Does your cloud provider have well implemented patch management  policies and procedures?

✓  Does the cloud provider have application level firewalls and other tools that help keep your application or code safe?

✓  Can the cloud provider keep security information such as private keys private?

✓  Does the cloud provider provide encryption and key management?

✓  Does the cloud provider have a well-defined, well-executed identity and  access management architecture?

✓  Has single sign-on been implemented for the customers of a cloud provider?

