CHAPTER VIII

INTERNET CLOUD SECURITY

WhoOwns Whose Information on the Cloud?

The user organization. The informa-tion elements stored at the cloud provider's site are those of its clients, its employees, and its accounts. If so, this is a flagrant case of absentee management because the least that can be said is that these information elements are not under their owner's direct watch but under somebody else's, that of the cloud infrastructure provider.

This curious reversal of responsibilities (which is accompanied by absentee accountability) brings up the second critical query: Is the provider assuming legal responsibility in case of identity theft, with all damages covered? As far as the cloud infrastructure is concerned, this case has not yet been tested in court, but other evidence from similar cases is disquieting.

When Responsibility for Security Takes a Leave, Accountability Goes Along

Current lack of security can get more than an order of magnitude more dramatic with the cloud. The way negotiations between cloud vendors and their customers shape up suggests that a user organization suffering severe damage from computer crime, while its database resides at the cloud providers infrastructure, will also be held responsible for it.

The level of security and access to the infrastructural services being offered depends entirely on the enterprise owning the servers. Therefore, the latter should also be legally responsible for security and protection associated with the services it provides. To appreciate why responsibility for security may be taking a leave, user organizations must understand that public cloud systems:

- typically feature access levels that are a sort of free access for all, and
- among subscribers there may also be potential intruders masquerading as legitimate users.

Theoretically, security purposes are served through a set of design principles and gadgets. The first allow us to define a framework for the effective application of tech-nology protecting privacy and security. The second are the gatekeepers. Practically, the nature of the cloud as an open resource

makes it very difficult to police applica-tions and customers by the hundreds of thousands and their whereabouts.

In addition, technology can be a double-edged sword, because design prin-ciples promoting security and those advancing the notion of a more effective, more flexible, and less costly system contradict one another. The benefits of effectiveness are numerous, including unprecedented interoperability of business systems and applications. These same benefits, however, work against greater security. Thererxist as well conflicts of interest in a business sense. *If the* cloud makes it easier for consumers and cheaper, too, as the pros say, *then* by significantly increasing the number of accesses, the likelihood of failures and fraud increases, too.

Eventually, everybody would get a "go" at the cloud as many services start being offered for free, supported by advertising.

If a cloud-based e-mail ser-vice sees to it that one does not have to worry about the bill (though somewhere this is going to hit its limits), *then* the real costs may be opaque, with violations of privacy and security becoming major cost items.

These *ifs* and *thens* are a concern not only to consumers but also to companies. Small and medium enterprises (SMEs) benefit by switching to cloud-based e-mail :>ecause accounting and customer tracking supports run inside a web browser. Also, :ne ability to summon computing and databasing capacity from the cloud, when needed, sounds great, but as the user population rapidly multiplies, security con-cerns start mounting.

Even if at least some consumers may be happier to trade a bit of privacy for tree services, when this "bit" grows in size, they will start having second thoughts. Though people appreciate a free lunch and don't object to listening to the ads, they also like to:

- have control over their personal data and
- be able to amend their profiles, which service providers compile and use to target advertising.

A private cloud is better positioned in security terms because it gives the user organization ownership of stored information and full control of how to structure the security service Still, the private

clouds' wide band connections to the public cloud emulate a multitenant environment, wh *it* the public infrastructure is under the authority of the service provider.

The reasonable thing to do, in order to confront the challenges posed by this case, is to have all cloud providers and all user organizations (or their ass ac-tions) get together to establish common standards for security solution unc: *u* new *cloud security authority.* This should be a state regulator who has full p: to inspect them, audit them, and police them. This is not even under discus-sion, leading to the notion that increased potential for fraud is to a large part due to:

- the absence of standard security practices, including their verification on the Internet and the cloud and
- legal and regulatory ambiguity and uncertainty with regard to application and jurisdiction of current laws and regulations concerning online activities.

User organizations, too, must become more realistic about security risks. Today several tend to disregard the fine print of security because they . - lidur databasing in the cloud to be convenient, and they also hope to control their IT costs this way. Of course, there is always a trade-off between security and convenience, operating cost, and certain factors relating to performance. The golden rule, however, is that:

- the level of security requfted should relate to the operational risk involved, and
- slack in security is essentially lack of care, which means that responsibility takes a leave and accountability goes along.

Data Fill the Air and Many Parties Are Listening

llu very strength of the Internet—its large communications system, pow-erful search engines, and any-to-any connectivity—facilitates its abuses by unscrupulous individuals, companies, and governments. The fact that much of modern business greatly depends on database mining and networked resources intensifies the problem.

The Internet's promotion of anonymity serves a purpose but also fosters abuses. Issues resulting from code breaking and defective surveillance have not yet found fully satisfactory solutions in terms of protection of privacy. To make matters more complex, protection measures have their

downside. Digital certificate infrastruc-tures bring up integrity problems, and new challenges have come from nonpropri-etary free software.

With the cloud the list of problems not in control keeps growing. Individual mobility by lightweight portable devices and sprawling wireless networks has been generally commented on as an important business advance. Somehow forgotten is the fact that wireless networks are notoriously vulnerable to hacking:

- their users will be well advised never to believe they are secure, and
- aware of this, many companies are now worrying about the challenge pre-sented by the growth of wireless networking.

Cloud computing finds itself at the middle of this worry. The concept of mobile and land lines in a networking sense is a commendable objective. But what's its effect on privacy and data security? The dependability associated with existing means for protection is very low indeed,^ practically reducing them to simple sources of evi-dence that "something" is being done.

New, more powerful means of protection employ analytical techniques. Introducers, however, also use similar approaches—and some of these introducers are no kids, but mighty governments and military alliances.

Denial of service attacks occur when a computer forces another to use up to saturation network resources or its own. This may take the form of forcing a host to respond constantly to a barrage of packets so that it cannot perform its formal functions, and neither can it let other packets through. Large information provid-ers have installed filters to identify forged packets often used in denial of service attacks, but there are no ideal solutions.

DDoS attacks are a real and present danger with cloud computing. Warfare, as well as terrorists and other criminals, may cut off the user organization's information lifeline by making IT services unavailable, extorting payments, or taking other mea-sures whose aftereffect is equivalent to a DDoS attack. It needs no further explaining that cloud security is a complex issue whose surface is just being scratched.