# Technical Risks

## Table of Contents

Cloud Computing Security .............................................................................................................. 2
Temporary Loss of Availability ........................................................................................................ 3
Permanent Loss of Availability ........................................................................................................ 5
Insecure Deletion of Data ............................................................................................................... 7
Data Leaks and Breaches ................................................................................................................ 9
Failure to Properly Isolate Data .................................................................................................... 11
Cloud Neighbors ............................................................................................................................ 13
Economic Denial of Service Attacks .............................................................................................. 17
Insecure Interfaces and APIs ......................................................................................................... 19
Vulnerability Assessments ............................................................................................................ 21
Notices .......................................................................................................................................... 22
**001 So what other technical risk? We'll cover each of these. Technical risks, we'll just, from a summary slide here, we'll just talk about CIA, right? There's a number of availability concerns that need to be addressed, confidentiality concerns, and who has access to view that data, what's the integrity, you know, how is that data protected within this environment? We'll cover each of these here on the next few slides.
Temporary Loss of Availability

Outages

- Previously local applications, are now subject to cloud provider downtime
- Can be caused by
  - Internet Service Providers disruptions
  - Distributed Denial of Service attacks
  - Resource exhaustion issues at the cloud provider
- Lead to economic losses for the duration of the outage and reputational losses into the future

Examples

- August 2008: Google Apps down 24 hours
- June 2009: Amazon EC2 down 7 hours
- March 2009: Microsoft Azure down 22 hours
- And many more…

**011 So temporary loss of availability, well there’s some examples on the bottom, where Google Apps was down for 24 hours. If your business is depending on the internet service provider, that software as a service provider, to actually do your core business functions, and it’s not available, that’s a problem. If Amazon’s EC2 server is down for seven hours in the middle of the night, and I’m running an e-commerce site on there, you know, I’m potentially losing some money from, you know, California, or, you know, if I’m selling goods to Europe. You know, I might not think it’s a big deal in the US if I’ve got an outage from midnight to two, unless I’ve got some kind of global operation, and then it does become a big deal.
So those are just a couple of things to keep in mind. We—in general, internet service provider disruptions, we've got nothing different than what we would have in our own environment, trying to get out from a business perspective. But now you're depending on the internet for your core functionality, whether it's your internal users going out to a site to run something like Google Apps, or whether it's running a critical service out there that customers are going to be accessing to, you're now depending upon a lot of things. Not just the cloud provider, but internet connectivity and other issues that might be going on. So keep those things in mind. Yeah, so a couple of things. The economic loss piece.

And that actually ties to a couple of things.

Just really understand your infrastructure and what your core businesses are. So how much can I afford to be down? What is one minute, or five minutes or one hour of downtime worth to me as an organization in loss of revenue, because that's what you're going to need to compute once your service provider fails and things don't work out, and your service is not available, you've got to be able to monetize that. You've got to be able to say that this outage cost me potentially 5,000 dollars or 10,000 dollars in potential revenue, because unless you can justify that in any way, you've got no real recourse. You've got nothing to go over to the service provider and say, "Hey, I want a 2,000 dollar credit, or a 5,000 dollar credit, or whatever it might be, you know, if it becomes a legal issue as well."
Permanent Loss of Availability

There is a dependence on the cloud provider’s disaster recovery procedures.

Lost encryption keys can make data useless.

Example:

In October 2009, T-Mobile Sidekick users utilizing Microsoft's Danger cloud service had their personal data lost, some without recovery.

**012 So permanent loss of data, or permanent loss of availability, I should say, hey, the idea here is, what if that service goes away? Now the T-Mobile Sidekick example is in here. It’s a neat one. There was a service that the T-Mobile phone essentially had its contact and address information stored on a server, by a service provider, the Microsoft Dangerous Cloud Service, the Microsoft bot danger, etcetera. But essentially there was a problem with that. Not only did that service availability, you know, go down, or the service was down, but there was damage, there was data that was lost. Some people lost contacts, they lost images, or because of poor practices on the back end, for getting things backed
So there’s this whole trust but verify model, you trust that your service provider, your cloud provider is doing the right thing, but you need to somehow verify that before it becomes an instance like this.

You also have to deal with the fact that, how established is that service provider? Amazon is probably not going away anytime soon, or Microsoft, for that matter, but some of these other smaller cloud computing service providers, they may or may not, so make sure you do your due diligence there.

Encryption is a big one. We talk about HIPAA policies in our policy module, where we’re dealing with health information data. We might be dealing with other PII or sensitive data or financial data that we don’t want people to have access to, whether it’s people coming through or accessing those resources over the internet, or our systems administrators or people that are managing that cloud environment, we want to make sure that’s protected from them as well. So maybe we’re implementing disk encryption or some sort of file encryption. How are we managing those keys, and what happens if those are lost, or were not properly being backed up. Certainly an issue.
Insecure Deletion of Data

How is data stored in the cloud disposed of when the customer no longer needs it?

- When a customer requests data deletion, true wiping may not take place.
  - Even if wiping is employed, some artifacts may remain.

- It is unlikely that the provider will destroy the physical disk that other customer's data may be stored on as well.

**013 Insecure deletion of data. I can't remember if it was 60 Minutes, or what it was, there was definitely a little news video on some copiers that were actually- non-cloud related, sorry, some copiers that had actually printed a number of confidential sensitive documents, and they're basically sitting in a warehouse, and these things are getting scooped up or bought, these refurbished copiers by people throughout the world, and they did a couple of tests of basically pulling out the hard drives and doing some quick forensics evidence on there, or forensics collection, and seeing that there's all kinds of documents that were not securely wiped off of those things.
It's the same type of thing that you need to worry about with your cloud service provider. If you're dealing with sensitive information, it has to get written to disk someplace, somewhere, and once it gets written to disk, once you're done with it, how is it wiped? How is it cleaned, right? So, you know, there are service providers that do adhere to NIST standards and guidelines for securely deleting or wiping data, but that's one thing that you need to verify with your service provider, that when you're done with your instance, you're done with your data, that it is securely wiped, whether it's virtual or physical, you want to make sure that that physical device actually gets rid of your data.
Data Leaks and Breaches

Data that was previously stored entirely locally is now being constantly transmitted back and forth between the customer and the cloud provider.

- Potential for new threats that were previously not an issue
  - Man-in-the-middle
  - Side-channel
  - Sniffing

There may be data breaches that the cloud provider does not notify the customer about to maintain the business.

No service is perfect and mistakes will happen:
*In March 2009, Google Docs inadvertently shared user documents with contacts that they did not authorize*

**014 Here we go. So data leaks or breaches. These are-- this is actually-- there's a couple of things that address this. The idea is, how independent are my virtual instances? And again, most of the bigger providers do a good job of isolating or sandboxing their-- your stuff from somebody else's stuff, and that's important to note. They have those different security zones for your particular instances that support you, but that's one thing that you need to-- again, trust but verify so that you don't have some of these side channel options, or you don't have the ability to sniff network traffic in your cloud computing environment, or if you have access to a machine and you're actually able to install Wireshark, or
tcpdump and you actually start to look at the packets in there, can you see other customers’ data? And that’s a concern. All right, it may be an unnecessary concern, depending on your service provider, but in some cases, it is a legitimate concern that you need to be aware of.

All right, the other piece to consider is, how are you connecting into your environment? Are you just, like I mentioned, remote desktopping into that environment, SSH into that environment, or do you have some sorts of VPN connection into that environment? If you’re using a VPN connection and you’re going from your corporate site into some other cloud computing environment out there, what sort of access rules are allowed through that VPN? You know, if I’ve got a piece of malware in my corporate environment, can it leak into the cloud? Can that data, the sensitive data that’s in the cloud leak into my corporate environment?

So you need to make sure that you take definitely certain care to control the firewall rules that support some sorts of VPN connection, and have some sort of intrusion detection things in place.

Yeah, the example there with Google Docs inadvertently sharing user documents, they-- they talk-- their justification was, "Well, it was only a few documents, and they weren’t spreadsheets, or anything important." I like their justification for that. Programming glitch with their security model, and their user permissions. Nice.
Virtualization hypervisors are used to manage and provide isolation between cloud clients.

- Flaws in these hypervisors can be exploited to allow the introduction of malicious code.

Improper permissions on data may allow one customer to view another’s data.

- Insufficient logging or auditing of access may leave these vulnerabilities unnoticed.

Guest-hopping, side-channel and other attacks are possible.

- Mostly theoretical…for now

**015 So failure to properly isolate data. What we have here is, we talk about problems within VMware, for instance, or problems within Xen. What is the hypervisor that’s in use? Are there vulnerabilities that let you break out of your virtual instance, and access a virtual instance or information off of another virtual machine. Is it possible? Yes, there’s a number of things out there. Some of it’s theoretical, but the idea here is, if you have-- if you require that certain level of protection, right, if you want that extra level of protection to say, I want to make sure I’m secure from somebody breaking out of the hypervisor to another virtual instance, does your cloud provider give you the option to have dedicated hardware? That
really mitigates that risk right there. For a little bit more money, I'm pretty sure most of them will do just about anything, right, but the idea is, do you have the ability to have dedicated hardware for your virtual instances to protect against something like, you know, this virtualization piece, to break out of virtualization? We'll see.

Improper permissions, well there's lots of different permission sets. It's who has access to my con-- Yes?

Student: This might be kind of unanswerable, but given, you know, say, I host my application, I'm responsible for application level, if that's hacked by whatever reason, and someone else is affected, where does, usually the risk-- or who's responsible for that? Is it cloud provider who should have isolated it, or is it me, because it's my application? And I know that's kind of--

Dennis Allen: Well, no, no, it's a very good question. So let me just make sure I understand. So you're saying, I have an application that's running in the cloud that somehow gets compromised, and because it got compromised, it was used to further attack somebody else.

Student: Yeah.

Dennis Allen: Okay, so there's actually an example of that coming up here.
Cloud Neighbors

Resource sharing means that if another customer of the same cloud carries out malicious activities and you can be affected as well.

Spamming, port scanning, or the serving of malicious content from cloud infrastructure can lead to:

- A range of IP addresses being blocked (including innocent tenants)
- Confiscation of resources due to neighbor activities

Example

- In December 2009, a command and control center for a Zeus botnet was found inside Amazon’s EC2 infrastructure.

**016 Oh, look at that, on our next slide. Cloud neighbors, right? So we talk about different things that could compromise our cloud environment, or impact our availability, so I’ll address that one in a second.

So since we’re all sharing resources, we’re sharing network resources, we’re sharing physical CPU and disk resources. What happens if somebody’s able to take all the CPU cycles off that physical box, impact my availability, right? What things are there to protect me against that? What happens if somebody consumes all the bandwidth, right? Now, whether it’s, they’ve got a high volume website, and all of a sudden, it slows yours down, that’s a
big deal. What happens if I have an application that gets compromised and somebody gets the Zeus botnet on there and-- or the command-- it turns out into a command and control server, so now all these bots are now talking back to my server for the command and control for the botnet.

Has it happened? Well yes, there's an example here of where an Amazon server was actually compromised. Are you responsible? Well you're responsible in that-- it depends on the application, right? So if you're running, you're handling financial data, credit, you know, credit card data, health information, depending on what regulatory compliance things apply to you, there are certain things you're responsible for, because now that machine has been compromised, what other things were compromised? Was it credit card data? There may be fines associated with that.

So in that regard, you're responsible. You're responsible in that you, as an individual, are not doing those sorts of things on purpose, so there may be acceptable use agreements that say, you're not going to be doing scanning sourced from your environment, you're not going to be trying to do packet captures, you're not going to be trying to run a botnet from your environment, trying to do something bad. So if you were doing that on purpose, there's some responsibility there, too. What you see in this environment is, Amazon says, "Hey, look, we were able to determine this, and as soon as we found out about it, we were able to shut that down, so they were able to mitigate that, revert it, or whatever they
needed to do. So in this particular case, it was really just Amazon talking about what a great job they did to detect it and shut it down as fast as possible. Not necessarily the repercussions on the individual that got compromised.

So are you responsible? It depends a little bit, but I mean, ultimately, yeah, you're responsible for making sure your business is running, and if it does get compromised, there may be other fines or something associated with that.

Now, so there we go. Oh, the one thing, the confiscation of resources, I think we have an example. I'm not sure if it's in another slide. We can mention it here. In Texas, there was a data center that actually had an incident, FBI came in, and they scooped up hundreds of servers. Now, not all of them were actually involved in the incident, and if-- it impacted other companies that were actually working out of that data center. So now, not only have you lost, you know, I mean, there's been an incident at the data center for where your stuff is being coloed, and you're obviously concerned about the best practices of your data center, that's one thing. Now you've physically lost your ability to conduct your business, because your virtual instance that was on the same piece of hardware, or even in the same location as somebody else's instance, has been scooped up.

Now what they tried to do is, they tried to get a restraining order on the FBI in order to try to get their data back, which did not work out, because I believe the judge said that there was probable cause for it
to be-- for them to actually confiscate all that hardware, which kind of put them in a sticky situation, because, you know, their business is down, right, they just-- Now the FBI was kind enough to clone their drives for them, and send them to them, so they can get their business up and running elsewhere, but you could see how that could be an issue.

We see that a lot. I mean, that's not just a cloud instance, or a cloud circumstance. When you're dealing with things that are illegal, and search and seizure laws, the FBI or whoever it is, could come in and confiscate your mail server, if there's child porn or some other malware on that mail server. If somebody has downloaded all kinds of illegal music, or illegal videos or whatever it might be, and it's on a production file server, law enforcement could come in and take that production file server and impact your business. So this is not anything not anything new to the cloud environment, other than the fact that you have very little control to what actually goes onto those physical resources.
Economic Denial of Service Attacks

A cloud customer’s resources may be used by malicious parties to harm the customer financially.

- An attacker can gain credentials for a customer’s account and use their cloud resources to damage the customer.
- A malicious user could use up the cloud customer’s metered resources.
  - Example
    A DDoS attack against a pay-per HTTP request site hosted in the cloud

**017 Second, economic denial of service. This is another one that we have to consider, and we are on this pay-per-use model. So if all of a sudden, my website was having a normal level of bandwidth and utilization, and it spikes to something that-- not necessarily that it can't handle, but certainly something that, maybe I can't afford, we might have an issue there. So we might essentially lose money there.

The other piece of this is, how can I leverage somebody’s credentials to set up my own instance. So you have visibility, you log into your console, you see I might have four or five different virtual instances set up. Can somebody
actually leverage those credentials to provision another instance and provide web services command and control for a botnet or some other production e-commerce services, whatever, but leveraging my account, and my credentials. That is a possibility in some cases. So protecting those credentials becomes a very big deal, and how do we do that, whether it's simple user name and password, or talking about X.509 keys, etcetera, there's different ways to protect your access to your account information. And that's where the role based access comes into play as well, right? We have certain people or logins that allow people to go in and provision new instances, or to configure firewall rules, all right, and they may be different than accounts that actually let people access their resources to configure an application within that instance, or something like that. All right, who has the ability to tune those sorts of things?
Insecure Interfaces and APIs

Cloud customers access cloud services using a set of management interfaces and APIs created by the cloud provider.

- These interfaces are Internet accessible, making them more susceptible to attack than in-house controls.
- The security and availability of the cloud service are dependant upon the security of these interfaces.

So insecure interfaces and APIs, application programming and interfaces. This sort of falls in the same lines with the user control. But who’s reviewing that code? Is that code outsourced? Is there some developer in another country that’s developing that middleware application that allows you to access your shared cloud volume or your shared cloud instance. Who actually looks at that code to make sure that it’s done securely? Because, as I mentioned, you have to have some way to access that. Now we talk about once the instance is provisioned, because we’re talking a lot about infrastructure stuff here. Once I’ve got a Linux box, or a Windows box, and I can access that directly, that’s one thing.
But how do I manage that? You know, how do I actually connect into that environment if I’m using some sort of custom application?

And if I am going to use some sorts of custom application to move volumes around or do backups or do some things like that, how am I passing those credentials? Are they going over https? Am I using any kind of user names and passwords in that programming, to actually access that instance? It’s an issue. It’s something that certainly needs to be addressed in terms of how you're connecting into your cloud environment to manipulate your instances, to bring them up, bring them down, etcetera. Now if you’re logging in right through, like the console, or the service provider, obviously you’ve got different features that are available to you and things, but a lot of people are writing their own custom applications to do those-- or scripting their own things, in their own environment to access those resources.

There’s tools like-- has anybody heard of RightScale? They are one of the leading providers, certainly in supporting Amazon. They’re looking to branch out to providing a middle wear piece, to manage-- to manage multiple cloud providers through one interface, to let you configure those security zones and create new instances. GridGain is another one that I mentioned the ability to maybe move instances from cloud provider to cloud provider. They're looking to use-- try to help establish some of the standardization-- things for-- standards for the APIs to be able to move things from cloud to cloud, and manage some of those instances.
Vulnerability Assessments

Because data is now Internet-facing, it is more susceptible to network based attacks.

- Most cloud providers are not going to allow an external penetration test to be completed by your company.

Regulatory compliance may require vulnerability assessments that now need to be completed by the cloud provider.

**019 So vulnerability assessments. This is a big one in your environment, if you’re dealing with PCI compliance, or just in general, trying to do regular assessments of your infrastructure, you know, there’s going to be some sort of external port assessment or vulnerability assessment that’s going to happen coming into this cloud instance. Is that a violation of your security policy? Am I allowed to port scan internally? Maybe I have my own vulnerability assessment machine internally. Am I allowed to scan my several different instances that are running in my own cloud from the internal aspects. So you’ve got to look at the acceptable use agreements, and work with the service providers to see what’s
allowed internally as well as what's allowed for people to do that assessment piece externally, and in addition to that, is there an onsite part of the assessment required? Depending on your environment and what your regulatory compliance might be, a physical onsite assessment might be necessary. Will the service provider let you come into that data center, evaluate the physical security controls, and things that are in place there? So that's one thing that you---you certainly have got to be aware of those types of things, and understand what the requirements are for your

**Notices**

© 2016 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.