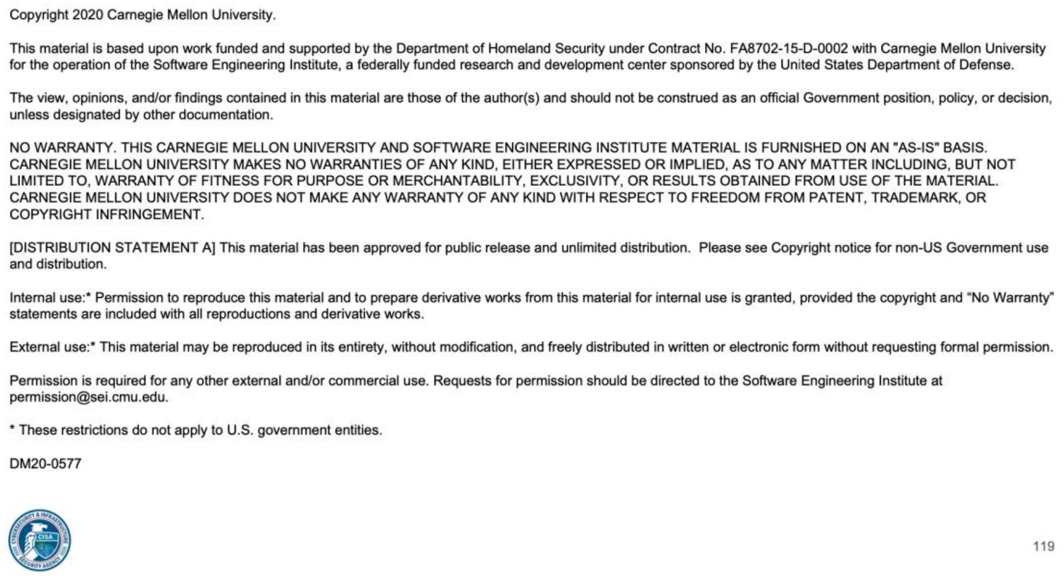
Security Guidance for Critical Areas in Cloud Computing Demo



Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission.

Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM20-0577

Instructor: In this video, we're going to take a look at the security guidance for critical areas of focus in cloud computing from the Cloud Security Alliance. This is a rather large document covering, as you see, fourteen domains. So, we're not going to get into every last detail, but what we will try to do is highlight a few elements that maybe weren't covered in as much detail in the slides or the other reference materials.

So, the first domain, cloud computing concepts and architecture, you'll notice down here for definition of a cloud computing model, it references the NIST definition, including the five essential characteristics, service models, deployment models, etc. You have a sample network diagram for infrastructure as service as well as a platform as a service and even software as a service.

This logical model is a neat one. As you see, we have a highlighted key point here. One of the key differences between cloud and traditional computing is the metastructure. Cloud metastructure includes the management plane component, so the idea that there is this metastructure between the underlying physical servers and networking etc. There's this metastructure that the cloud service provider maintains, but they also, through that, make certain things available, like software defined networking that you would need for virtual private cloud, that type of thing. So, how did they make those services available to the customer in an infrastructure as a service type of environment?

And, of course, they get into the shared responsibility model, and, depending on what services you are taking advantage of, infrastructure as a service is mostly you, the customer, software as a service, mostly the provider.

And we've got other security models and our cloud security process model as well. What I have highlighted here in the security process model is that you see where implementing controls is. It's farther along in the path. You need to make sure you identify your requirements. Select your provider based off of those requirements and your needed deployment models, and then define your architecture and access controls, figure out where your gaps are and where you're going to need to develop some compensating controls, and design those, and eventually you get to actually implementing them before you do your change management and go into production software. So, there's a lot of planning that needs to happen up front before you get into the cloud.

Domain two, governance and enterprise risk management, one of the key points here is that contracts are their primary tool for governance between the cloud providers and the customer. So, even if they don't have a default one, it's important that you come to your cloud provider when you're subscribing for services and you let them know what you need, what you need for your organization in terms of incident response, support, service level agreements, compliance and regulations that apply to your business, and then they may have things readily available to support that, but then they also may need to customize it to support your needs. So, developing that contract is really that focus point to guaranteeing success.

The key point here that we want to highlight for reviewing audits and assessments to ensure they're up to date really means that you need to make sure you're not just doing this once. This is, at a minimum, an annual process where you're going to evaluate these policies, these contracts, and make sure everything is in place, perhaps even exercise them as part of your incident response plan.

Third domain, legal issues, contracts, and electronic discovery, the biggest takeaway here is, in many cases, you're dealing with different countries that might have different rules, and those really apply to the location of the cloud provider, their home base. Their headquarters might be someplace, and there's applicable laws there. The user itself might be somewhere accessing the cloud provider, the organization, etc. The data subject, if you're handling hard data or health information or whatever it would be for the service that you're providing, they may be in a certain area. European Union with the GDPR is going have certain rules and regulations that apply to those subjects. The servers themselves may be in different locations, whether they are in Europe, or in the United States, North America etc., There's going to be different rules that apply for those. So, it's just understanding that there are many elements to your cloud solution, and they may be distributed globally. So, you need to understand what rules and regulations apply to those locations.

This document does a good job of highlighting some key points for each of the regions. We won't go into each one of them, but you can see here they've got Australia, China, Japan, Russia etc., a little bit more about the general data protection regulations, GDPR that I mentioned a moment ago, etc., as well as the Americas. So, there's some very specific guidelines that they have for cloud services in those regions. So, it's a good resource for you.

From a forensics standpoint, a bit by bit image of a cloud data source might not be possible. You're dealing with a multi-tenancy environment. They may have multiple customers that have data physically on the same drive. So, if you were to image that, there could be some bleed over. So, there might not be the same opportunity to recover those deleted files from slack space and whatnot that you normally would be able to get in a traditional digital forensic scenario.

Compliance and audit management, this is a neat diagram down here in the left. It builds on top of certified services. So, think about this. The service provider has to apply some regulation or standard such as ISO 27001. They have to apply that to auditing and implementing controls within their infrastructure. So, that scope is one hundred percent the cloud service provider, but then you're building upon that with your own custom applications, which also need to be compliant for your needs. So, if there's an application that you're building that fails to meet this compliance, then the whole thing is out of compliance. So, keep that in mind. These pieces build upon each other in the shared responsibility model, and, if there's a gap in one, it could lead to a compromise, fines, etc.

Information governance, again, we get into a number of details here. We'll highlight the data security lifecycle. So, you need to prepare this for your environment. Just understand how it works and then how you would apply that to a cloud environment. So, data has a lifecycle in which it is created. Where is that stored? How do you define access control lists for that storage? Who has the right to access it or use it, if you will, and then can you share it? Is it publicly accessible to the world, or is it restricted use on a need to know basis, that type of thing? And then eventually, is it archived? Is that part of a backup process? Is it part of an archival to meet your own compliance or standards for keeping data for X number of years, and then eventually, it's destroyed, and is it destroyed securely? How is it permanently wiped from that physical drive?

And then you get into domain six, management plane and business continuity, and one of the biggest takeaways here is to always architect for failure so that whether that is using auto scaling groups for load balancing and to be able to ensure you have enough resources to accommodate the demand or multiple zones in case you have a geographic disaster, hurricane etc., you might want to have compute zones that are on opposite ends of the country or even different countries altogether. And then, of course, the risk-based approach that we see over here on the right. The idea is not all data needs to be treated equally or assets for that matter. So, your level of protection should be commensurate with the value of that asset. So, if you're dealing with media files like that you would have publicly available on YouTube, you don't necessarily need to have the access control lists or have them encrypted because you're essentially giving those away, which is different than, say, trade secrets, which you'd want to make sure you have very strict access controls on and have them encrypted in transit and have them encrypted at rest, and there might be, again, regulations that might apply to payment card data, health data etc. So, your approach to spending money and control implementation really needs to be appropriate for the value of the asset that you're trying to protect.

And our example here on the right is a sample hierarchy, if you will. So, you'll have a root or master account, which, once you get set up, you want to minimize that use, but you still need to admin like activities. So, creating a super admin or a couple of super admin accounts there for specific users is going to be appropriate. And then from there, you'll have administrators for various services, whether that is a web application service, a compute resource, a storage service etc. And then inside of there, you might actually have the service, maybe it s a developer updating code, or it's people that have access to upload files or download files, that type of thing. And then where possible, especially with any kind of privileged access, you want to implement multi-factor authentication.

Let's take a quick look at infrastructure security. So, the key point here that's being highlighted is that, if possible, you want to run all applications on their own virtual network. So, this is a little bit different from the DMZ model you have. In the traditional DMZ, you would have your web mail and DNS all kind of lumped together on that one virtual network that your firewall provided access to the world, and you were filtering out just specific ports to those hosts. Well, in this case, it's almost like having a virtual firewall per device or a host-based firewall. So, you want to configure this isolation at the application level as much as possible to limit an attacker's ability to pivot, and there's no cost to it. That's the magic piece here. It's not like we're buying a new firewall device to do the separation. It's really just software defined networking and access control lists and taking advantage of the services that are already there to add this extra layer of control. So, it might be a little bit more complex, but it Doesn't cost you any more financially to do it and for the added benefit of more security.

So, when we look at workload security, there's this concept of immutable workloads. So, in here the idea is that you deploy an image that cannot be edited. It can't be updated. So, it goes away. When it goes away, a new version of it might get spun up, or you might have multiple instances of this immutable image in order to support scaling and the demand, and you don't really need to access it. So, you can disable remote logins because it's a standard service that goes through this lifecycle, as we see over here on the right, where you go through the configuration management, and you're pushing out the source code, and you go through all of your various security tests. And once that's approved, you're updating the master image, and that master image is the one that gets automatically pushed into production. So, you don't really need to access that master image. What you would essentially do is blow it away. You would remove that instance from production and deploy the next version of that image, and, therefore, you're less worried about what's actually running or the life and the maintenance of that running system because it never runs that long.

So, domain eight, virtualization of containers, there's just a couple things to mention here. It's important to understand that the cloud provider is responsible for that compute virtualization layer. So, that virtualization infrastructure and enforcement of isolation, that is their responsibility. There's obviously a lot more information within the guide.

Domain nine, incident response, there's a couple key points here. There's another reference to a NIST document here, 800-61, which talks about incident response. And just as an overall takeaway to this Cloud Security Alliance guide is it's just a really good cybersecurity best practices. Now, it has a cloud twist to it, right. It's how does it apply to the cloud context, but, overall, it covers a lot of bases in cybersecurity. Here's just another example of that as it touches upon the incident response lifecycle. And a good thing is, from a forensics or incident response perspective, having a cloud jump kit is identifying those tools that you need inside of your cloud environment to pull down logs, to do that analysis offline, to do that image. Is there a way to extract that image out of the running compute infrastructure and then pull it offline to do an additional investigation? So, coming up with what that forensics process is and what tools you need to do that is paramount. You don't want to do that during an investigation. You need to have that all planned out ahead of time.

And an important point here is, during your investigation, you always need to make sure that that management plane or that metastructure is free from an attacker. Certainly, if it's compromised in some way, then that attacker could then pivot to other customers and whatnot. So, that is something that you need to coordinate with your cloud service provider. As soon as you detect something like that, you need to let them know because they're going to have incident response procedures in place to deal with something like that as well.

Application security, we'll just touch on one big thing here. Make sure you're using secure software development lifecycle within cloud computing and with everything you do. So, again, it's another good point about this document is that it's introducing a lot of best practices for cybersecurity in general, not just cloud computing. So, you have some introduction to secure software development, talking about design and secure operations and references to Microsoft security development lifecycle as well as some NIST guides and open web applications security project, OWASP.

So, you got some design concepts here that takes you through that lifecycle on the various phases, which is kind of neat. And similar to our immutable workload diagram, you have the idea of going through your configuration and code development, checking that into a repo, but then you're doing all your tests, your security tests, your functional tests, your nonfunctional tests, and then once you have an approved application, then you're preparing it for production.

So, data security and encryption, it's interesting to understand the different types of stores that exist in the cloud. Object storage, typically files, but they might not be in the format that you're used to, clear text, files. They might be log specific files, API specific files, that type of thing that the cloud interface reads, and you just need a place to store them or that they could be archived offline and adjusted into another tool. Buy-in storage is your typical hard drive that gets attached to a virtual instance, and then there's this concept of application or platform storage. CDN is a good example of that. Your content delivery network is an application that you're using to push out those files to the edge.

So, identity and access management, or in this case identity entitlement and access management, they get a-- this is a pretty neat statement here. As Gardner defines IAM, " A security discipline that enables the right individuals to access the right resources at the right times for the right reasons." So, that pretty much sums up IAM in one sentence for you.

Security as a service, this is one of the last domains here in the Cloud Security Alliance guide. It really just touches upon some of the benefits and concerns when leveraging a security as a service provider. So, they have the staffing expertise. That's their job. They do it for a living so they know the ins and outs of it, and they may even know how to implement their tools in the cloud, the cloud that you're using. So, that level of expertise saves you the time to learning it, and you have a presumed level of confidence and expertise that they have. And then related technologies, there's a whole other domain here in the Cloud Security Alliance Guide.

So, that's a very long comprehensive document. It's a great resource to have available to you. It goes into much more depth than we have here in this cloud security course. So, I'd highly recommend you to check it out.