Good evening, thank you for inviting me to join this distinguished panel. I was asked to talk about virtualization and cyber-security. Starting my career at NSA, security has always been a fundamental part of everything I have done over the years.

As you heard from my introduction, or read in my biography, I have numerous years of experience as a government decision maker that chose and financed many technical initiatives supporting the Department of Defense and Intelligence communities. Now I am in the commercial world driving the R&D of future technologies and building the technology solutions being implemented in government and the commercial sectors. In both roles the cyber-security challenges I have faced are the same. We have to take the approach of building, what I like to call a "Smart Infrastructure" where security is horizontally integrated throughout the development, and not just differed to an IA checklist that is reviewed during fielding.

At EMC we have made a substantial investment in the areas of virtualization and cyber-security. Back in 2004 we acquired a small company called VMWARE which leads the marketplace in virtualization, and in 2005 we acquired RSA Security the industry leader in security products. Since then we have been building these two capabilities into every thing we do at EMC.

Lately I have spent a lot of time in the areas of virtualized environments and cloud computing

Generally I speak to customers on the benefits of cloud computing, like: the value, efficiency and dynamic capabilities these architectures enable. But for this conference I want the audience to understand the cyber implications of cloud computing and virtualized infrastructures. If you remember nothing else I say, remember that:
Cloud computing is changing the dynamics of cyber security

Through proper implantation and management of virtualization technologies, many of the security vulnerabilities we have in traditional architecture designs are mitigated, however a new set of challenges are introduced.

I could really go on and on about how cloud computing works, or even just the security aspects of it, but given only ten minutes I really just wanted to highlight some of the security aspects of cloud computing and get the message out that Cloud computing can enhance security, or if improperly implemented and managed, it lead to greater security risks, either way, it is: **changing the dynamics of cyber security**

The first thing I would like to talk about is the idea of Scale-Out Compute Utility, virtualization or even Cloud.

You may not realize it but the idea of scale out utility has been around for half a decade. In fact it started in DARPA back in 1963 with a little program called Multiple Access Compute (MAC). Since then for the last 50 years the IT industry has simply been updating the MAC.

The latest version, cloud computing have brought sophisticated automation, provisioning and virtualization technologies that have significant cyber security implications.

Before we talk about how secure these environments can be we must be honest with ourselves and recognize that all the risk we know and love still exist and in-fact with cloud we expand that risk beyond the typical boundaries that we know today. We are actually increasing the attack surface or creating new ways to attack IT assets.

Because of this we must look at security in a whole new way.

There is no more Point to security anymore. Today's world of sophisticated malware, targeted threats, and multi-stage attacks require security that is smart, cross-linked and interoperable. We must adopt an information centric approach to security and move beyond the traditional disparate reactive defenses that form a broken safety net made of point security tools.

On one end of the spectrum we have Identities, those people and processes that should or should not have access to system resources. On the other end we have information which must be accessible or restricted however the organizational policy directs.

In between these two environments you still have the brick and mortar. The applications, servers, networks and storage still exist. In today's model you have system administrators at each layer of the technology stack configuring or miss-configuring their components and maintaining that environment ensuring they have the latest and greatest security patches that rarely come out.

Industry must develop and deliver technology components that support centralized, consistent management of security across the technology stack.

According to Sans, the number one cyber vulnerability is unpatched systems. Just think about that….this means, thousands of compromised systems, loss of information, man hours lost due to recovery, and of course the effects of having information compromised (military operations, loss of lives, loss of identity, loss of funds,….) All completely avoidable if only the systems were patched. Forget about the threat of the expert state sponsored hacker, unpatched systems leave us vulnerable to every script kiddie out there.

I would like to finish by taking a look at some of the principles of this information centric environment.

The first principle is that it must be dynamic and intelligent. The static, reactive environment that we have today will just not work. Capabilities like adaptive authentication that are behavior based mechanisms to determine assess to resources must be utilized.

This is not a new concept, in-fact it is used across the financial industry today. If you have ever had to put your zip-code into the gas pump when outside you typical travel patterns you have used this technology.

This environment must be transparent to the enterprise and the user. Security can not be an after thought; it must be embedded in the fabric. It must be built into the products and infrastructure by the vendor community. Far too many products that I look at today take 40 bit commercial encryption from the internet engineer it into their products and claim they have secure products. At RSA we provide the BSAFE tool kit free of charge. By using this we and our competitors can build secure products that meet FIPS140-2 encryption standards.

It must be Risk based and business aligned. Security must be driven by flexible policy that is aligned to the business or mission need. The need for a common framework to ensure that security policies are consistently applied across the infrastructure is critical to the success.

And finally it must be Holistic and Layered. Security must be able to be enforced wherever the information lives. From endpoint to datacenter integrated and consistant across the technology stack.

Thanks you for your time!