



The Security Division of EMC

RSA Conference 2010

March 2, 2010

Good morning, everyone. Welcome to RSA Conference 2010.

This gathering becomes more important each year.

More than just the occasional story of a database breach, cyber vulnerabilities and attacks are topics in the main stream media as never before.

Underlining the criticality of the situation, this week you will hear from Secretary Napolitano, FBI Director Mueller, White House Cyber Security Coordinator, Howard Schmidt and a host of industry and Government Leaders.

It just never seems to get easier for us as vendors and practitioners... does it?

Malware at pandemic levels, a global economy struggling to recover in a strait jacket of cost controls and a new wave of computing struggling to take hold – cloud computing.

But it could get easier.

How?

By leveraging the technologies enabling the cloud to secure it.

Sounds heavenly.

But as my father used to say: “Everyone wants to go to heaven but nobody wants to die to get there.”

And because cloud computing represents a challenge as well as an opportunity.

We have to be careful we don’t end up in security hell!

Whenever I feel boxed in by a big challenge, I like to look to history as a reminder of the boundless creativity of the human mind and its ability to completely re-imagine aspects of life that to others seem unchangeable.

We don’t need to look any farther than the recent past and the man we honor this morning, Whit Diffie as well as our own “R”, “S”, and “A” for this kind of creativity in their re-imagining of cryptography.

These are people who see what others before them cannot—no matter how hard they look.

And from their insight, they build a new vision—sometimes quite literally.

Consider another inspiring example.

Imagine what it was like to live as a blind person during the three centuries following Gutenberg’s invention of the printing press.

The printing press represented a sweeping transformation of the information infrastructure of the time.

It changed forever the way thoughts, knowledge and information were shared.

And yet if you were blind you would have been locked out of this new world of recorded knowledge.

Then in the early 1800s along comes Louis Braille - blind since the age of three.

As a 16 year old, he envisioned and then devised a system that would enable the blind to write as well as read.

His curiosity led him to a form of communication used by soldiers on the battlefield at night when they needed to send written messages to each other ... but didn’t dare light a match.

Braille adopted their grill of raised dots ... but dramatically improved and simplified their system ... and it persists today.

As one historian put it, “Braille was the Gutenberg of the blind.”



The Security Division of EMC

How does this relate to our industry and our situation today?

I believe, we in the security industry need a more elevated and expansive vision connected to the huge wave of IT transformation under way right now that is Cloud computing.

Think for a moment about why cloud computing is so powerful.

It enables businesses to leave their aging, inflexible, and costly IT infrastructures behind and move to a new “pay as you go” world characterized by choice and agility.

And not a moment too soon, because organizations are spending as much as two-thirds of their IT budgets just to maintain their infrastructure and applications –keeping the lights on.

Cloud computing can dramatically alter this two-thirds / one-third ratio ... so that much more energy and investment can be directed toward real innovation and competitive advantage.

Trouble is something’s holding back the full realization of this cloud vision.

And that in a word is security.

CIO Magazine recently published its state-of-the-CIO study.

And get this, 51% of CIOs surveyed – more than half – cited security as their “greatest concern surrounding cloud computing adoption.”

And if your suffering from cloud fatigue or are tired of hearing about it, let me remind you of the then MIT Media Labs visionary, Nicholas Negroponte, who said in 1997:

“The internet is the most over-hyped but underestimated phenomenon in history.”

Mark my words, the same will be true of Cloud computing.

Cloud computing will complete the transformation of IT infrastructures unleashed by the internet.

Organizations will demand it because they absolutely must get faster and better returns on their IT investments.

So we must play an essential role in making cloud computing a reality.

Here’s the scope of our challenge and our opportunity as I see it:

The challenge is to ensure that safety is designed and built into the cloud so that organizations of every size – from the smallest merchant or agency to the largest government or multi-national – can make broad use of the cloud... fully confident that their information and transactions are secure.

Our industry needs to deliver security services that ensure levels of protection in the cloud that surpass what physical environments offer today.

In short, people everywhere must be able to trust the cloud even if they literally and metaphorically can’t see it.

That’s our challenge.

What about our opportunity?

The answer is that cloud computing is going to make your work more important and prominent than ever before.

Cloud computing is our opportunity to turn the way we deliver security inside out.

I say that because the cloud will force organizations to pay serious attention to their security management processes not just their endpoint – dead endpoint - security technologies.

We have the rare opportunity for a “do over”, to be present at the creation and roll out of this new wave of computing with security built in from the get go.

We can be in on the ground floor to create an infrastructure that is actually more secure and more enabling of innovation than today’s physical infrastructures!



The Security Division of EMC

That's my focus today – how together we can make the cloud inherently secure, compliant and governed in a manner that ensures the confidentiality, integrity, and availability of our information.

In other words, security that enables business like never before.

So where do we start?

In the world of cloud computing... we will need to enforce all of the same identity, information, and infrastructure policies we have in the physical world.

But it gets trickier because virtual infrastructures decouple your software environment from its underlying hardware infrastructure... so you CAN aggregate many servers, storage systems, and networks into shared pools of resources.

As we consider how to make the cloud safe I think it's best to begin with people, process and technology – just as we do in other aspects of business and security.

So let's start with people and process.

In the physical world these are siloed.

Separate groups focus on storage, servers, networks, endpoints, and so on.

In the cloud, many of these operations and roles will converge.

For example, we're likely to see virtual machine administrators who are playing all the roles of network, storage and server administrators simultaneously.

This convergence of roles brings new challenges... We'll need to rethink policies and related processes for handoffs between security teams responsible for governing information infrastructure and operations teams that ensure quality of service.

Let's hear more on the topic of virtualization from Paul Maritz of VMWare.

[VIDEO]

Virtualization is the engine of the cloud that will propel us forward; not in one sudden, giant leap, but rather as a journey that organizations will take at their own pace, realizing tangible benefits at every step along the way.

And by embedding security in the virtual abstraction layer - we get our "do over"!

We can enforce policies for information, identity, and infrastructure within this virtual layer.

As a result, we can shift from infrastructure to information-centric policy concentrating on what is most important -- the information and who gets access -- rather than on a meaningless perimeter or mere plumbing.

We see four, well-defined stages on this journey...

The journey begins with virtualization of non-mission critical infrastructure like test and development systems and low risk applications.

According to VMWare statistics about 25% of servers are virtualized today and many of your organizations are well into this phase by now.

There are relatively few new security requirements at this level given the non-critical nature of the applications but it is in this stage that you will become adept with the tools of virtualization and begin the process of "hardening" the virtual infrastructure.

In the second stage of the journey organizations virtualize critical business applications.

Here your infrastructure becomes far more scalable and elastic with the security requirements scaling in proportion.

You will need the same level of visibility for compliance in this virtual environment that you had in the physical.

Here, insider risk increases in importance given the portability of virtual machines.

And it's at this point that we'll want to push security down the stack, deep in the virtual layer.

Embedding controls that today are bolted on to the physical infrastructure.



The Security Division of EMC

In the third stage of the journey... the enterprise begins to develop internal clouds and operate their information infrastructure as a utility.

This stage consists of a fully virtualized and automated data center where application workloads are policy- and service-level driven.

Now, the enterprise must have far more mature processes for Governance, Risk and Compliance that can span their physical and virtual infrastructures.

And because of the convergence of roles I spoke of earlier (server administration, network etc.) monitoring and controlling privileged access becomes increasingly important.

Additionally self-service and self-provisioning add new levels of complexity. So monitoring and controlling changes here will also be critical.

In the fourth stage, enterprises start to outsource their infrastructures to external service providers. But you won't want any part of that unless service providers can demonstrate their ability to effectively enforce policy, prove compliance and manage multi-tenancy.

At this stage, federation becomes an important capability.

Organizations will need the ability to dictate and federate identity and policy to their service providers on how information is accessed and handled.

Next they'll need to demand that cloud providers deliver strong proof of compliance, even in the deepest levels of the cloud.

Service providers should be able to tell compliance officers and auditors just about anything they need to know – with verifiable metrics.

The ultimate goal is to generate a concise summary of relevant events occurring in the infrastructure that feeds directly into a GRC dashboard that visualizes the state of compliance.

The last element in this fourth stage is how the multi-tenant environment is managed.

Service providers must defend against co-mingling the sensitive data of multiple tenants.

To achieve isolation requires controlling the flow of information between the tenants.

To do this we will need to create pools of trusted resources or zones.

These trusted zones will be directly managed by the virtual infrastructure that ensures the enforcement of information policy within and between these zones.

But sometimes you just don't want the same two tenants on the same physical machine. For example I can't imagine Coke would ever want their virtual machines on the same hardware as Pepsi's.

To achieve this will require innovative thinking on how we in essence reconnect the physical to the virtual world.

This can be accomplished by leveraging a hardware root of trust at the chip level that verifies virtual machines are running on the right hardware systems.

Hardware roots of trust could also be leveraged to create trusted pools of systems with similar security profiles or compliance requirements, that can then be dynamically allocated to optimize workloads.

These trusted pools of cloud resources really become the best of both worlds:

they provide the fluidity and flexibility of the cloud with the assurance of predictable, proven security controls and processes.

This capability... to achieve visibility to infrastructure as a service, assess the security posture of that service, trust the resulting measurements and prove compliance to auditors is not just theoretical.

This morning RSA announced a collaboration and proof of concept with Intel, VMWare and the newest addition to the RSA family, Archer Technologies, demonstrating exactly how this visibility can be accomplished and you can see the proof of concept in the EMC booth focused on Accelerating Your Secure Virtualization Journey.

While the advent of cloud infrastructures built on a measured chain of trust is not a cure-all for cloud security and compliance, it does mark an important milestone.

The hardware and virtualization layers, formerly a "black box" within the cloud, now become as inspectable, analyzable and reportable for compliance as the cloud's top-most application services layer.



The Security Division of EMC

With this previously unimagined level of visibility, cloud providers can develop the infrastructure-level policy controls and end-to-end security attestations to handle the most demanding security requirements.

So those are the four stages that represent the journey but the larger point here is that we do know how to surmount these challenges.

Let's hear from Dave Cullinane, Chief Security Officer of eBay sharing his unique perspective as a practitioner, cloud service provider and founding member of the Cloud Security Alliance.

[VIDEO]

By now, two things are clear. The journey to the cloud is inevitable and we're going to have to secure it.

But the fact is, we're being presented with an opportunity to advance information security beyond anything else since the advent of encryption!

Cloud infrastructures will catapult us forward because they force enterprises to focus on their security policies and processes – and not just on security technology.

Think about it—if we can get security built into the virtual infrastructure from the get-go ... we can not only have visibility and manageability but risk decision points, and controls everywhere.

In short... the cloud will turn the way we deliver security inside out.

And Information Security will enable cloud computing to take full advantage of the Internet turning our current IT models inside out as well.

This means we can deliver new waves of efficiency, agility and collaboration for organizations of all sizes.

Yes it will be challenging, but history reminds us that we've managed through other sweeping transformations from the physical to the virtual world.

I'll leave you with this example.

Consider how our monetary system evolved.

We started with barter—my chickens for your grain.

Coins made money more portable—but you still had to carry your actual wealth with you.

Paper currency began virtualizing wealth.

These promissory notes with no intrinsic value required us to start dealing with the concept of attestation... certifying that something is genuine or true.

The banking system brought service providers into the mix. Credit Cards. ATMs.

And with the advent of financial instruments—bonds, stocks, mutual funds, etc.—we found ways to share wealth so that when one party wasn't using it, another could.

Sound familiar?

Of course, virtual money has dominated the money supply for decades.

And, along the way we had to think about standards, regulations, federation between organizations, and more – all because money must be based on trust.

Now, no system is perfect.

Every system has its abuses and unintended consequences.

But would we ever go back to trading chickens for grain?

Not likely.

Cloud computing will indeed complete the transformation of IT infrastructures unleashed by the Internet. As security practitioners, we must lead, not follow.

And after 15 years in this industry I know we've got what it takes to embrace the challenge and seize the opportunity.

Good luck along the journey and here's to a great conference!