Good morning everyone.
What a great start to our 20th annual conference.

My congratulations to Ron, Adi and Len for your tremendous achievements, and my personal thanks for your inspiration over the years.

That was a wonderful tribute, Jim, and all of our thanks to you for organizing and launching this conference in 1991 and for your outstanding leadership over the years.

Your contributions are why our Lifetime Achievement Award is named specifically for you.

Thank you Jim Bidzos

We have indeed been fortunate to stand on the shoulders of giants.

But it would be unlike us in this conference or as an industry to be too self-congratulatory or self-important.

We know all too well, we are only as good as the last attack we have withstood.

And let's face it, while we have relied on numerous "giants" over the years to create the success we've had, we've also had to navigate our way around a few pygmies.

That's why I thought it might be entertaining for you all to hear some of the titles and content from past presentations that turned out to be less than prescient and, occasionally, with 20/20 hindsight, downright comical.....

As I looked through our archives of photos and conference brochures, I have to say there was a wealth of material.

When delivered - some concepts seemed to make intuitive sense but never achieved escape velocity and failed to reach ubiquity.

Take smart cards, first mentioned in 1994 (we were minimalists with our marketing brochures then).

By 1997 we were talking about incorporating PKI into smart cards.
We should have been nervous that same year, though, because we featured a track on how to crack a smart card.

By 2000 the handwriting was on the wall with “Do PKIs Need Smart Cards? What’s the Next Best Thing?”

The abstract read: “How can we secure the PKI if smart card readers don’t materialize everywhere?”... Good point.

How many of us have smart card readers eleven years later?

And although, as Jim said, we have been spectacularly successful implementing Public key cryptography, embedded in SSL... applications... and hardware too numerous to mention.... massive public key infrastructures were a different story. ....Let’s take a look.

Here’s a graph of the number of track sessions offered on PKI by year.

We seem mired in the trough of disillusionment.

A closer look will help us understand why.

In 1999 we had our first warning that it might not all be heaven: “PKI Integration – It’s Not All or Nothing”

It was also the same year that “Uncle Sam Meet the PKI” How’s that HSPD 12 working out?

I myself wasn’t immune from the hype serving in 2001 on that ‘legendary’ panel – “The Year of PKI” with John Ryan from Entrust, Fran Rooney from Baltimore Technologies and Stratton Sclavos from Verisign.

....Ah, memories.


You know it’s over when you have to reinvent it.

While smart cards and PKI never achieved the ubiquity we thought, they’ll continue to play a
major role in security.

But there were also some of those ‘what were people thinking moments’.

Can any of us forget the clipper chip and key escrow? ....Neither one of those was funny at the time.

How about 1995’s “Public Key and the US Postal Service”.

And proving that neither rain, nor snow, nor common sense kept our postal service from its online rounds, they followed up with 1997’s “Postal Electronic Commerce Services”.

Fortunately, the world didn’t go postal.

Another few ideas whose time never came: 1996’s “Encryption on the Fly for Windows 95”

and the memorable -
- listen to this --

“Public Key for Single Sign-On in Distributed Computing Environments” -- a three time loser.

We’ve also had a few Jerry Springer moments along the way.

Who could forget the panel with Kevin Mitnick, seen here with Chris Painter, his prosecutor and his antagonist Ira Winkler.

I thought for sure chairs were going to fly and we were going to hear chants of...... Ira, Ira.....

Now check out the snake in the background photo peering menacingly at Mitnick– now look at Ira.

... Who’s scarier? Yikes.

Once, the RSA Conference organizers were even physically threatened for allowing Frank Abegnale to tell his story “Catch Me If You Can”.

We are nothing, if not passionate, in our loathing for our adversaries.

And how about the time when the father of the Internet, Al Gore, was heckled and shouted at from the audience.
And Al, a man of peace.

And as competition to speak to this audience has intensified over the years, we have seen the
titles of abstracts get more outrageous in author’s attempts to get the committee’s attention.

Some are silly or clever: “Cloudy With a Chance of Litigation”;

“What Happens in Vegas Goes on U-Tube”?
“Queer Eye for the Chart Guy”;

“Papa Gino’s Secret Sauce For Next Generation Hardware-based Security”.

....You couldn’t make this stuff up.
But wait, there’s more...

Some are violent:
“Zombie Trojans Throwing Spears”,

“Sex, Drugs & Cybercrime: Go Flux Yourself”,

“UTM Smack Down” and

“Die Script Kiddies Die, Die, Die”.

Some even have sexual overtones:
“The Dirty Little Secret of IAM”,

“The IT Security Industry – Geeks Gone Wild”,

“The Case of Promiscuous Parameters”, and

DOD SOA Gone Wild!
A Look at the Horizontal Fusion Initiative”.

And finally there have been countless Now What’s, Best Practices and Lessons Learned.

Each year we have more than 2,000 talented, creative individuals vie for 200 speaking slots.

As I say every year, they are the backbone of this conference.

And kidding aside, their content is illuminating.
....We appreciate them all.

Well, I hope you enjoyed that look back as much as I did.

To paraphrase the philosopher George Santayana: ‘Those who do not study and understand the
past will be condemned to relive it’.

And, while I don’t think we should take ourselves too seriously, we should also be very proud of what we have accomplished.

Learning from our successes and failures, building on the rich heritage of our giants, we continue our important work and with an eye to the future.

Abraham Lincoln once said that ‘the best thing about the future is that it comes only one day at a time’.

Having presented at this conference for over 10 years, I have the luxury of reflecting on the results of that daily progress each year in this keynote.

With my colleagues, I do my best to craft a vision for our industry, using the privileged insight available from so many of you to challenge us to jump ahead and intercept the future – to see things as they might be – not as they are.

Reflecting on recent conference content and keynotes:

We now recognize the limitations of perimeter defenses and the need for information-centric security has become conventional wisdom.

We now acknowledge that to be information-centric, security controls must be more intelligent, flexible and dynamic – “Thinking Security”.

We now understand that security budgets are finite and that to be cost-effective, security infrastructures must be grounded in a thorough understanding of risk, balancing the elimination of threats, with probability and materiality.

We now know a criminal ecosystem has developed and that nation states and non-state actors like Wikileaks pose new threats that can only be countered with our own cooperative ecosystem.

That despite day-to-day competition vendors must integrate technologies…. industries must share best practices and threat intelligence….and governments must cooperate with one another and the private sector.

And last year, the rallying cry from my keynote was “safety in the cloud” and the chance for a “Security Do-Over.”

So this year my theme is “Trust in the Cloud?”

I know what you’re thinking.
...Is this going to be another series like the year of PKI?

The answer is not really, there is a difference.

Last year my keynote was about the promise.

This year it’s about the proof.

The promise is that you CAN achieve safety in the cloud.

The promise is that we CAN fundamentally do security differently and better.

The proof comes when, by leveraging virtualization technology, we demonstrate better control and visibility, the key elements of trust, in cloud environments.

At this point, the IT industry believes in the potential of virtualization and cloud computing.

IT organizations are transforming their infrastructures which means we’re well on our way to an era of “applied IT” where investments will focus less on infrastructure and more on leveraging IT to solve higher level business problems.

But in any of these transformations the goal of security remains the same - getting the right information to the right people over a trusted infrastructure in a system that can be governed and managed.

But independent of this transformation to cloud we’re seeing an enormous amount of change across the dimensions of information, identities and infrastructure -- creating a nightmare of control problems and visibility issues...The antithesis of trust.

First, we have a tidal wave of information being created and more and more sensitive information being shared.

This creates significant information governance challenges regarding where sensitive data moves, who gets it, how it’s protected at rest and in motion, how, in a world of replication, we delete it, etc.

Second - Identities are proliferating.

In addition to our traditional internal users, we have customers, partners, a growing number of mobile workers using consumer devices and even machines, accessing our infrastructure and information.

Everyone and everything needs access.
Third - The entire IT stack is **changing**.

We now have a virtual layer that abstracts the underlying storage, compute, and network infrastructure.

Our boundaries become logical rather than physical.

Our workloads now move, so we can no longer depend on the physical infrastructure as a proxy for the information or process we are trying to protect.

And as the endpoint splinters into a thousand variations, the IT team is losing control and visibility over that too.

There are two other dimensions of change.

Threats have shifted from viruses and malware to more Advanced Persistent Threats, and "low and slow" crimeware making static policies and signatures all but useless.

The same is true for insider attacks.  
There's no virus signature for a crooked database administrator.

Compliance also continues to evolve with more regulation.... more changes within regulations....and greater reporting requirements.

Considering all the challenges created by these changes, it may at first seem that virtualization and cloud complicate the problem.

It’s widely reported that confusion and fear are holding organizations back from adoption.

But deliberately or not, organizations are already moving to the cloud in response to business demands.

Fearful or not, these changes are making cloud adoption inevitable.

Pardon another historical reference but it reminds me of the time before Columbus – a world brimming with opportunity beyond the horizon but unexplored because of dangers that may have lurked past where the eye could see.

And just as reaching the east by sailing west was counter intuitive....It may seem counter intuitive to use the technology enabling the cloud, virtualization, to secure the cloud.  
But we can....
In other words, virtualization is our silver lining in the cloud. Alright, penalize me ten yards for shameless use of a cliché...

But if leveraged properly virtualization can also be the pathway to surpassing the level of control and visibility that physical IT offers.... transforming the infrastructure itself into a vital resource for improving security and compliance in three striking ways.

First..... Security becomes logical and information-centric.

In virtualized environments, static, physical perimeters give way to dynamic, logical boundaries defined by information and transactions.

Logical boundaries form the new perimeters for trust, and virtual machines adapt security to their particular workloads, carrying their policies and privileges with them as they travel across the cloud.

Second.... Security becomes built-in and automated.

In clouds, where information, VMs and entire virtualized networks relocate in the blink of an eye, security measures must be just as dynamic.

Achieving this means building security into virtualized components and, by extension, distributing security throughout the cloud.

Also, automation will be absolutely essential to enabling security and compliance to work at the speed and scale of the cloud.

Policies, regulations and best practices will be codified into security management systems and enforced automatically, reducing the need for intervention by IT staff.

And third...... Security becomes risk-based and adaptive.....because static security approaches can’t address evolving threats.

In the near future, trusted clouds will employ predictive analytics based on their understanding of normal states, user behaviors and transaction patterns to spot high-risk events and allow organizations to proactively adapt defenses.

Adopting these principles enables a heightened level of control and visibility that will lead to trust.

While I’ve advocated for these principles in the past, we are now at an inflection point where they are being applied in solutions arriving in the market place.
To make this tangible, and to share proof rather than just promises, I’d like to invite Richard McAniff to the stage.

Richard is Co-President and Chief Development Officer of VMware, and our teams have been hard at work over the last year building on our collective vision of the secure, trusted cloud.

WELCOME RICHARD

Art: Richard, I want you to get to those proof points.... but before you do, can you give us the VMWare perspective on the journey to the cloud that’s underway.

Richard:
We’ve done a lot of research within our customer base, and we see three distinct phases as companies move toward the cloud.

The first phase is where companies discover virtualization and recognize the cost savings associated with consolidating multiple physical servers onto virtual servers.

Often the non- critical workloads are virtualized during this phase of the journey.

After you are about 30% virtualized, we see that the drivers behind virtualization start to change.

In the next phase, the key driver is resiliency.

While consolidation is still very important, themes like up-time, high availability, back-up, and disaster recovery emerge as drivers.

In fact, one customer recently told me that he didn't care what the hardware consolidation ratios were.

Even if he didn't save a penny on capex, keeping his critical applications up and running alone is enough to justify any expenditure on virtualization.

And of course, especially with this audience I would be remiss if I didn't talk about security and compliance which become critical in this phase.....

In fact when I meet with customers security is probably the most talked about topic when it comes to moving to the cloud...

Getting back to the journey....
If phase 1 is being driven by capex.....and phase 2 is being driven by resiliency.....then the third phase is being driven by agility.

We call this phase of the journey.... cloud computing.

Inside the firewall, we call this a Private cloud....outside the firewall, we call this a public cloud.

Art: Let me follow that up........
Do you agree, as I suggested earlier, that regardless of fear and uncertainty, organizations are moving toward cloud adoption?

Richard: We do.
Business owners are demanding that their IT partners be more responsive to their business needs.

More and more information is being collected, and business owners want access to that information.

They don't want to wait days or weeks or months for a new machine to be provisioned.

They don't want to wait weeks or months for an application to be built and deployed.

We are all being conditioned to expect that with a click of the mouse we will get the resources that we need.

If I can download a new app to my iPad, why can't my IT organization provide me with the same level of service?

And while we are just beginning to see infrastructure delivered as a private cloud, we are also seeing more and more SaaS applications coming into the enterprise.

And these Saas applications represent a potential security hole that I'll talk about in just a minute.

In fact I'd like to challenge everyone in the audience to write down exactly how many SaaS applications you think you have within your enterprise, and then go back and see if you are correct.

Don't worry, this isn't a quiz, and you won't be graded, but you may be very surprised ..... I certainly was when I did this exercise myself.

In fact, Saas applications remind me of how PCs entered the enterprise back in the late 80s...in a very viral fashion.
And just as windows PCs provided tremendous productivity gains, they also caused a lot of problems that we are still cleaning up today.

Art: Now let’s talk specifically about how virtualization changes security......

Richard: First, as you pointed out, security systems today are built on the notion of a static infrastructure, and applications are attached to this static infrastructure.

Virtual machines however are by nature dynamic: adjusting to load, memory usage, storage, compute and networking requirements as defined by an SLA.

We call this elasticity and this notion is a fundamental building block of what it means to be a cloud infrastructure.

This also means our approach to security has to be fundamentally different.

Second, if security is built around the notion of pooled physical hardware: IP addresses, port groups, machines and so on...it becomes very hard to translate business policy into security rules without creating thousands of them.

When you have this many rules it becomes very difficult if not impossible to automate them.

That is one of the key messages that you touched on just a bit ago....it is critical that we automate many of the security policies...especially in a world where applications can migrate from one data center to another at the speed of light.

The key to automation is to simplify these rules by translating business policy that connects applications with end users.

We want to eliminate the need to translate business policy based on physical resources or physical machines.

Last, cloud environments are typically about new boundaries.

In a shared infrastructure, you may be sharing with another tenant.

You can no longer clamp a physical box onto a cable.

When you are dealing with multiple tenant environments where applications can move around dynamically, as I said, you need a different approach.

Art: So with that as a backdrop, let’s get to those proof points.
I see you have an illustration here.... Let's get our monies worth out of this Telestrator.

**Richard:** One of your 3 new dimensions of security was "logical information-centric boundaries.” Last year VMware introduced a technology called vShield.

What's exciting about vShield is that it enables organizations to "zone" their virtual infrastructure, and apply policies consistently across those zones.

Think of those zones as the logical boundaries you spoke of.

An exciting project we've been working on together is building some of RSA’s DLP technology into vShield, to enable information classification and discovery throughout the virtual infrastructure.

This will enable organizations to take an information-centric approach to zoning their infrastructure.

Imagine your infrastructure telling you; "here's a suggested zone for PCI, or PII or PHI".

That truly is an intelligent infrastructure.

**Art:** So, we’re making great headway to create these dynamic, logical boundaries.

But to create a true ecosystem what other security and infrastructure vendors are you working with?

**Richard:**

Again, vShield has given us the opportunity to build security controls into the infrastructure.

As I mentioned, we'll be doing that with RSA DLP. We’re also working with Intel to ensure a trusted vSphere platform.

The vShield platform enables embedding security controls at application, logical network and VM boundaries.

We are working with vendors like Cisco and HP to embed network security, or vendors like Trend and Symantec to embed endpoint security.

We are also embedding your access control technology.

And there will be much more to come.
At the same time, we’re working with RSA to simplify the management of those technologies and build them right into our management consoles.

A big element of this is the automation of management. RSA had some great proof points with that, did they not?

Art: Yes, we got a great reception at VMworld this summer when we announced our Solution for Cloud Compliance.

For those of you who did not see it, we developed 130 security controls for the virtual infrastructure using VMware’s hardening guide.

We then mapped those controls to a comprehensive database of regulations and security frameworks that reside within the Archer eGRC platform. An example is the PCI standard.

Archer discovers the status of the controls at the control management layer.....in this instance the compliance performance of vSphere is exposed through vCentre and read, interpreted and reported on by Archer.

We intend to expand integration at this layer to include other products such as McAfee’s ePolicy Orchestrator.

Finally, we've also embedded the matrix of controls from the Cloud Security Alliance within the Archer platform.

This allows us to measure cloud service providers compliance against benchmarks created by the industry.

These solutions will simplify the process of creating and maintaining secure and compliant clouds.

Richard: But how about risk-based and adaptive approaches, we still have work to do there don’t we?

Art: Yes, we're already adapting our risk-based authentication for verifying users in high-risk transactions and detecting fraudulent users inside virtual cloud environments.

And don't foget DLP is great for locating information at risk and, by policy, adapting the application of specific controls to facts and circumstances.

We also believe, over time, that we'll be able to extend our risk engine and behavior analytics to information and devices.
While these are not proof points this year, they will give us something to talk about next year.

Now Richard.... You talked about SaaS applications, and how they represent a security issue. - Talk a bit more about that.

**Richard:** That's right - SaaS applications are becoming more viral within the enterprise.

At VMworld, Paul Maritz, our CEO, mentioned that we had 15 SaaS applications, and he joked that he didn't approve any one of them.

I did a check last week, and it turns out that we now have 29. Think about this for a minute.

First, it probably means that most companies have multiple passwords floating around that are not tied into internal infrastructure.

If you use AD, it is very unlikely that they are tied into AD.

Now here are a couple of problems....aside from the fact that you may have a lot of unprotected passwords floating around, you are also probably putting mission critical data into the cloud without appropriate controls.

Putting data into the cloud isn't the problem....it's not knowing what is out there that is the problem.

Another potential problem is when an employee leaves the company....if the Saas provider has control, you will not be able to de-provision the user...

After they leave they still have access to this information.

Another issue, not completely related to security, is around management...you don't know how many licenses you are paying for.

At VMware we've been working on ways to solve these problems.

In fact, last year at VMworld we announced Project Horizon, an advanced development effort at VMware with the mission of delivering simple, secure end-user access to applications and data across a wide range of devices.

Project Horizon will broker user access to applications, virtual desktops and data resources, while preserving the required level of security and control needed by a modern CIO.

We think that Project Horizon is a game-changer.
And we are excited to be working with RSA on the new Cloud Trust Authority that I think you are going to talk about now.

**Art:** That’s right. When organizations leverage cloud services, they operate under a promise of security and compliance, rather than proof. That must change to truly enable trust in the cloud. But the challenge isn’t simply providing that visibility and control, but doing so across multiple providers.

Because organizations will likely partner with multiple SaaS, PaaS and IaaS cloud providers, it would be useful to achieve control and visibility without having to implement multiple point-to-point integrations to achieve that goal; hence, the introduction of the RSA Cloud Trust Authority.

Provided as a set of cloud services, the Cloud Trust Authority leverages technology from RSA and VMware and will provide visibility and control over Identity, Information and Infrastructure.

To meet the requirements of so many providers and customers this also means we will have to build up an ecosystem of security and infrastructure partners...

Like yourselves, Cisco, Intel, Citrix and others.....

The first version of this service, which will go into beta in the second half of this year, will enable a series of identity and compliance services.

The Cloud Trust Authority will be important not simply because of the services it will provide, but in how it will enable a more effective ecosystem of trust between enterprises and service providers.

**Richard:** That sounds great Art. I think together we’ve given the audience a lot to think about.

Thanks for giving me a chance to join you.

**Art:** Thanks Richard I appreciate you coming onstage to share your insights and proof points.

I think it was important for the audience to hear the views of security in the cloud from the leader in virtualization.

I hope you can come back next year and deliver your own keynote on virtualization.

Trust in the Cloud. It IS achievable

Not just in some distant future - but as these proof points demonstrate.....TODAY.
You may wonder if upon reflection 20 years from now, these ideas will stand the “RSA Conference Retrospective” test of time.

I think it’s pretty clear as we look at the trends we’re seeing in IT and in the marketplace, that virtualization and cloud will indeed dramatically and positively shape the evolution of security in the years to come.

I look forward to watching that evolution unfold and hope the coming years also provide some entertaining material for the next 20-year review, whoever gets to deliver it!

Thanks and have a great conference.

====================
RSA Conference 2011