



The Security Division of EMC

Art Coviello

A Common Call: Architecting a New Information Security Landscape

Keynote Transcript

RSA Conference 2009

April 21, 2009

RSA Conference - San Francisco, CA.

Good morning and welcome back to the RSA Conference.

This is the largest gathering of security professionals in the world, but there's another group of security experts whose members are not represented here today.

Or are they?

This group has more members than we have attendees; in the tens of thousands.

Its members collaborate across the globe offering each other diverse services.

They operate an effective and very profitable business ecosystem.

You've probably guessed by now that I'm referring to professional cyber criminals.

Technically adept, their fraud ecosystem is marked by innovation and agility and is highly opportunistic.

So yeah, they probably are here.

This group enjoys some unique advantages.

Unlike you, they are not bound by any rules of law.

They are not bound by service level agreements beyond the "honor among thieves" they share.

And, they are not bound by governance and regulations.

But they are organized, purposeful and effective.

They control massive armies of zombie computers.

They update them with the latest malware variants so their attacks can evade anti-virus signatures.

They collaborate, both offline to build their attacks, and in real time to launch them.

Their supply chain is amazingly sophisticated. They each have highly specialized roles.

And, even though they prefer to be anonymous, they've found ways to create relationships to build their supply chain.

This is what we are up against!

The situation is clear.

Our adversaries operate as a true ecosystem that thrives through interdependence and constantly adapts to ensure its growth and survival.

For us to succeed against such advantaged adversaries, the vendor community must take the lead.

Because technology is such an overwhelming requirement, we are the only ones in a position to build a security ecosystem.

But we must evolve from acting independently to solve discreet information security problems to acting collaboratively to create a common development process.

A process that ensures we are far faster and more flexible than the criminals.

So today I want to talk to you about how we can build a truly robust security ecosystem:

How not only the criminal threat but two other major forces are creating the need and opportunity to rethink the way security is developed and implemented; why we need a common development process to support information risk management; and finally, how the vendor community can collaborate to make it happen.



The Security Division of EMC

Let's start with what we already know about healthy ecosystems.

They are by necessity, not choice, interdependent.

When an ecosystem is threatened, its participants work together as a functional unit to protect the overall health of the system.

Like the introduction of a pollutant to a natural ecosystem, fraud threatens the viability of the entire information ecosystem.

So fraud is the first major force driving us to adapt and evolve.

A second and equally pressing force is the economic crisis.

While in some ways, technology contributed to our economic collapse by enabling levels of speed and complexity that obfuscated risk, technology also has the best potential to fuel our economic recovery.

Business, political and economic leaders alike look to technological innovation to drive the productivity gains and cost efficiencies that will restore economic growth.

But, rather than enabling this growth, today security is viewed as costly and ineffective.

Finally, the third key force is the rapid transformation of our information infrastructure enabled by emerging technologies now taking center stage.

Virtualization, consumerization of IT, social networking and cloud computing are being adopted at far higher rates than anyone ever expected.

At first because of the cost and productivity benefits; but increasingly organizations are attracted to the agility and new possibilities these innovations offer.

However, unlike the first two forces, this infrastructure transformation offers an opportunity as well as a challenge.

To better understand that opportunity, let's put this transformation into the context of our ecosystem metaphor.

Every ecosystem has an anchor.

In aquatic ecosystems the anchor is the ocean, lake or pond.

In a land based ecosystem the anchor is the soil.

And for our ecosystem, the anchor is the information infrastructure itself.

Swift adoption of these newer technologies brings us to a critical inflection point -- a point where we not only have the opportunity to restructure the information infrastructure almost from the ground up, but also have the chance to learn from past mistakes.

When you think about it, our current infrastructure evolved with no overarching design or master plan.

No process.

As new technologies emerged they were stacked on one another leading to what one IT executive refers to as a "leaning tower of technologies on the brink of collapse."

Perhaps this is overly harsh given all of the productivity we have gained from IT. I just think that we can do better.

And the same is true for security technologies.

Two years ago I talked about the disappearing perimeter and the need to protect the information itself -- an information-centric approach.

Even though we're doing a better job of that, security technologies are still applied piecemeal from multiple vendors -- cluttering the information landscape -- leaving perilous gaps of risk.

And that's where the opportunity lies for us to do better.

We must embrace a common development process that allows us to clean up this landscape, creating a more secure infrastructure today.

Then, with an eye to the future, we can ensure that the new technical infrastructure is designed around that process, rather than forcing a process around a collection of technologies.



The Security Division of EMC

So how do we create this development process?

By remembering the goal is to facilitate information risk management which ensures our ability to effectively balance the competing concerns of risk and reward, security and accessibility, and investment and return.

This process has four basic service functions.

1. Policy Management for defining and managing security rules that describe how our system should be governed.
2. Policy Decision points that determine whether and where security policies are at risk of violation.
3. Policy Enforcement for applying controls to prevent policy violations.
4. And Policy Audit for real-time monitoring and proof of policy compliance.

In some form or other most security products perform all four functions

However delivering and replicating these functions within individual point products hampers the dynamic management of risk and prevents us from applying security in the context of behavior -- content and real-time knowledge of the risk environment.

One of the reasons why the fraudsters are so successful is they poke at the infrastructure until they find a weakness in the system.

Today's security products tend to protect an element of the infrastructure from a defined set of threats, so what do fraudsters do?

They just work around those products.

The real breakthrough in overcoming the criminal threat and reducing skyrocketing costs comes when we decouple these individual functions.

This enables products to cooperate across infrastructure boundaries and vendor offerings as a system.

Let me show you how this can work.

By decoupling policy management from independent point products we enable consistent application of policy across any part of the infrastructure.

Key management is a good example.

While encryption products might contain some built-in key management capability, decoupling this function through enterprise key management streamlines the application of policy.

Next, by decoupling policy decisions from policy enforcement, we allow the selection of an enforcement control to be made based on context.

Consider adaptive authentication where we evaluate the level of risk or "trust" that a user is who they say they are.

This gives us the context to select an appropriate control from a range of controls striking the right balance between security and accessibility.

By decoupling policy enforcement from the application and building it into the infrastructure we breathe new life into controls making their application far more intelligent.

We transform static controls into dynamic, thinking controls that can be linked to each other.

Imagine your Data Loss prevention system being able to automatically trigger either desktop file encryption or Digital Rights Management, based on the type of information or risk.

Seamless...

Transparent...

Efficient...

and Effective.



The Security Division of EMC

And finally, by decoupling policy audit and monitoring from individual point products, we obtain a correlated view of information, identity and infrastructure controls -- gaining a holistic view of risk.

No one wants to know if just one particular point control is working and compliant, they want to know that their entire security system is working.

They want to identify all the gaps and have the ability to remediate.

What if your SIEM application could correlate data from Information controls like Data Loss Prevention; Identity controls like risk-based authentication and infrastructure controls such as patch, configuration and vulnerability management?

With this combined intelligence you could see a SharePoint site that not only contains highly sensitive unencrypted information but is running on a server that hasn't been patched in a month and a high risk user is accessing the site.

Very powerful!

In the web 2.0 world, we have seen the power of mash-ups -- so why not in the security world?

Ultimately, decoupling doesn't mean that point products get stripped of functionality.

Rather, they retain their unique and specialized role in the context of a larger system, leaving core shared functions to be applied broadly.

This makes the products within the system interdependent and allows the system to adapt to circumstances.

This is the very essence of an ecosystem.

Decoupling offers the promise of truly revolutionizing how we design technology and implement security.

Because of its Flexibility...Strength....and Tight Integration.

The resulting ecosystem will allow us to innovate with confidence, reduce the costs of security and beat the criminals at their own game.

Now, let's take a look at how we can get this done.

It cannot be solved by a suite of products from a single vendor.

The problem is simply too vast and the range of technologies too broad.

It must be solved by the vendor community and demands that we collaborate in new and far more constructive ways -- what I call inventive collaboration.

Inventive collaboration is about taking the discrete knowledge and expertise of one technology organization and inter-weaving it with that of another.

So here's the call to action.

We, as vendors, need to seize this opportunity in the following three ways:

First, although almost a cliché, we must collaborate on standards.

An example is the Key Management Infrastructure standard that EMC collaborated with HP and IBM to establish.

But the pace of standards development is often slow, especially in new technology areas -- causing standards to devolve into the lowest common denominator.

They are important, but cannot be the sole focus.

Second, we need to share technology.

Making core technologies in key areas more accessible can accelerate the growth and productivity of the ecosystem -- by reducing the time and expense of developing mature enterprise-class capabilities.

This is the reason RSA will make technology tools generally available over time.

The first of these was announced this week.



The Security Division of EMC

The RSA Share Project offers our BSAFE toolkits free to developers and invites them to participate in an online community with some of the greatest minds in cryptography.

Third, and most important, it will take enhanced technology integration.

Because information moves everywhere, the problem must be solved across the infrastructure.

That's why policy decision and enforcement points must be embedded into the infrastructure itself.

This is the reason that EMC, Cisco and Microsoft joined forces in the area of Data Loss Prevention.

By embedding our DLP technology into their products, we take a giant leap forward in clearing the landscape of point tools, creating a common language of policy and risk.

But perhaps the most exciting of these integrations is virtualization.

By embedding policy, controls and audit into the virtual layer now we avoid having to build a process around the technology and enable virtual environments to achieve near ubiquitous coverage in a frictionless manner.

As EMC's security division, RSA is working closely with our colleagues at VMware and others to do just that.

Our goal is for customers to gain the efficiency and flexibility of virtualization across their entire enterprise; surpassing the security models that exist in a purely physical infrastructure.

In fact we'll be previewing new offerings for security in a VMware environment over the next few days.

Paul Maritz, VMware's CEO would have joined us this morning but VMware is making a major announcement in just 45 minutes.

Instead, I have a short clip to play of Paul, sharing his views on security and collaboration.

I'd like to thank Paul for being virtually here....

I think you will hear many vendors echoing those comments about collaboration.

As a matter of fact executives from Microsoft and Cisco will join me on stage in a few moments to talk about their views on collaboration.

But that's the vendors. What of the practitioners?

I believe all of you will be saying its about time.

Finally....security embedded in and working across my infrastructure - an ecosystem to counter the fraudsters.

Finally...security applied seamlessly, transparently and cost effectively. And,

Finally....more time to understand risk, develop policy and work with business partners to enable innovation.

Let me conclude with a few last thoughts.

Industries often evolve in a linear manner, through a constant stream of incremental improvements.

Occasionally, just occasionally, industries experience a quantum leap.

Some tipping point changes evolution into revolution.

I suggest we are on the verge of such a tipping point.

We have the chance to not only change the game, but to win the game by creating an ecosystem that capitalizes on a shared development process fostered by inventive collaboration.

It is true that many of us are competitors, but this is not at odds with healthy collective transformation.



**The Security Division of EMC**

We're simply changing the basis of competition from feature wars, to an ability to work in and augment a system.

Vendors must take the lead but practitioners must demand this of us.

Never has there been a more exciting time to be working on information security.

The challenges are great, but if we collaborate effectively we can repel the cyber criminals we can reign in spiraling costs and we can reignite innovation.

There's an African proverb that advises, "If you want to go fast, go alone; if you want to go far, go together."

Thank you.

Two critical partners working together with RSA are Cisco and Microsoft.

Please join me in welcoming Brett Galloway, Cisco's Senior Vice President Wireless and Security Technology and Scott Charney, Microsoft's Corporate Vice President of Trustworthy Computing.