Deloitte.

Critical Partnering - The Global Enterprise Role in Cybersecurity

EastWest Institute

First Worldwide Cybersecurity Summit

Subject to Delivery

James H. Quigley
Chief Executive Officer
Deloitte Touche Tohmatsu

Dallas, Texas
May 4, 2010

Good morning, and thank you, chairman Finlay for that kind introduction.

General Jones—I'm certain I speak for everyone here in thanking *you* for your time, your insight, and your deep commitment to ensuring the world is fundamentally safer for all of its inhabitants.

My organization, Deloitte, is actively engaged in shaping the discourse around Cybersecurity on a number of levels, throughout the world.

Lt. General Harry Raduege, whom some of you have already met, spearheads many of our initiatives as Chairman of the Deloitte Center for Cyber Innovation and Mark Layton heads Deloitte's Global Risk Services practice. I'm delighted they are both with us today.

This morning, I would like to add a few thoughts to our collective conversation, speak about the Global Enterprise role in Cybersecurity, and look at that role from three different perspectives:

- Where does the international business community stand relative to understanding Cybersecurity as a risk?
- What is the unique relevance of that risk to the Global Enterprise?
- What kind of integrated response to that risk is warranted, if not demanded?

As we heard at last night's dinner, and the excellent panel discussions, there is a wide range of awareness and understanding of Cybersecurity as a risk.

Probably the *safest* comment I could make today would be to tell you, "OK, sure: the global enterprise agrees that there is a general, pervasive need for a deeper understanding about Cybersecurity, and for more education about it."

Or I could tell you that we're all in the same boat together.

But this would shortchange two realities: First, the international business community is, with a few exceptions, lagging the international military and political sectors when it comes to addressing Cybersecurity—even in industries that *know* about the risk.

For example, Deloitte's 2009 Global Security Survey of the Technology, Media and Telecommunications industry found 60% of responding IT leaders believe they are "falling behind" or still "catching up" to known security threats.

That's *worse* than the 49% who felt this way in the previous year's survey.

That's not good.

And the second reality is: "being in the same boat" is a small comfort if it's without oars, rudder or sail.

So let's take just a moment and ask why much of the global enterprise is behind the curve on Cybersecurity.

I believe it's because the Cybersecurity threat is both a relatively new risk classification and one that is growing and changing so quickly it's almost like a cancer: it can spread dangerously and require continual and sometimes aggressive treatment.

And we haven't figured it out the way we like to figure things out: with rigid assessments and diagnoses, with precise definition and nomenclature, and with clear processes and proven tools.

So, yes: I would say that the aggregate global enterprise is committed to gaining a deeper understanding of Cybersecurity risks.

But a commitment to awareness and education is only a small first step. And that brings me to my next point:

The unique relevance of Cybersecurity risk to the global enterprise means that we—the international corporate sector—must be advocates for change and action, and we must shoulder a large share of the responsibility for the overall response to the threat.

The battle will not be ours alone—we'll get to that in a minute—and there's no question that global co-ownership across political, governmental, geographic, and business interests will be essential to meaningful progress.

But let me share three reasons why Cybersecurity risk is critically important to international business:

1. One: Information is our de facto global currency
2. Two: Private industry has significant ownership of and responsibility for the global information infrastructure
3. And three: Cybersecurity risks threaten the productivity and competitive gains that technology investment has enabled.

Let's take those one at a time.

To say that information is the currency of international business is just another way of stating the obvious: in a global marketplace, the flow of virtually all goods and services is uniquely tied to the flow of information about those goods and services.

When you ask Fred Smith, the founder of FedEx, what kind of business he's in, he doesn't tell you that he runs a courier or package-delivery firm. He'll tell you that FedEx is in the information business—and that the information about a package's origin, location, destination, delivery time, price and costs are in many ways more important than the package itself.

Today, with hubs in Tennessee and Texas, and Guangzhou and Paris, FedEx moves about three-and-a-half million packages and 10 million pounds of freight every day.

You may think that's a lot of packages, but it's also a lot of information. And last month, when an erupting Icelandic volcano shut down air travel in Europe for a week or more, think about the value of that information to FedEx, its customers, and its brand.

Or consider any large consumer retailer, from Pantaloon, India's largest retailer, to Wal-Mart, with stores and operations in 15 countries, from Brazil to the United Kingdom, and joint ventures in China, Mexico and Japan.

Almost everything about their operations—from inventory to supply chain to transaction processing is linked and tracked and acted on digitally.

If you haven't had a good e-based shudder lately, Google "bar code scam"

and "Target" or "Home Depot" or "eBay." You will find scores of stories about how amateur, mom-and-pop criminals have bilked firms out of millions of dollars, using primarily a photocopy machine, a glue stick and a lot of nerve.

In one instance, cashiers were scanning expensive electronic equipment, like iPods, that carried a doctored bar code for $5 dollar headsets.

Another example that some of you may already know involved the discount retailer TJX, the parent company of such stores as TJ Maxx, Marshall's and HomeGoods.

In a significant data breach, lasting over 18 months in 2006 and 2007, 45 million credit and debit cards were stolen from its systems by an unknown number of intruders. This resulted in huge financial problems, bad press and significant down time for the parent company. TJX reported that it had set aside $118 million dollars to cover the cost of settlements as a result of its lax security.

In my business, professional services, the relationship between value and information is practically symmetrical.

And much of the information at the foundation of our work is confidential and proprietary, relating to fundamental business processes, capital market transactions, reporting and strategy.

So if the information is compromised, the relationship with clients, and alongside it, the reputation of the enterprise, is compromised.

My point is: whatever business you are in, from finance to entertainment to energy, you are really in two businesses. The one it says on your business card, and the information business.

And for the international enterprise, information is the global currency.

Unfortunately, the bad guys know this: In 2008, the global costs associated with stolen data were estimated at $1 trillion dollars.

And that figure may be grossly underestimated.

Research that Deloitte published relative to the *2010 CSO CyberSecurity Watch Survey* concludes that cyber crime is a more common and larger threat than is generally realized, and that criminal innovation and techniques have outpaced traditional and current security models and detection technologies.

I'm sure many of us have received the annoying letter or the disturbing phone call from a bank or agency seeking data verification or inquiring about a financial transaction. Or we've had to make our own discovery: just last month, my wife called my attention to a number of bogus charges on an HSBC credit card.

The second, uniquely relevant characteristic of the Cybersecurity risk to global enterprise has to do with private industry's significant investment in, ownership of, and responsibility for the global information infrastructure.

In the United States, industry owns an estimated 85 – 90 percent of the critical telecom-datacom infrastructure, including almost all of the wireless infrastructure.

For many of you here today, representing the Cyber40 nations, the percentage of privately owned or partnered infrastructure is also high.

And even where there is significant government control or ownership of infrastructure assets, there are almost always private-industry interests and touch points, including e-commerce, licensing opportunities, collaborations in research or manufacturing, and investment and funding interests.

But the ultimate relevance of Cybersecurity to private industry isn't about the satellites we've launched, the networks we operate, the cables we've laid, the towers we've built or the technologies we have developed.

It's about what these things have created for us.

Value. Competitive advantage. Insight. Innovation.

The potential for better products and services. Better processes and better governments. Better schools. Better hospitals.

Productivity improvements, and improved standards of living.

When you look at all the gains of productivity worldwide and the increased investment in IT in the last 20 years, there is a clear link between the two.

Dozens of papers have examined this, including one published by the Federal Reserve Bank of New York, asserting that virtually all of the gains in U.S. productivity in the late 1990s were linked to industries that produce or use IT most intensively.

Others have questioned the connection between IT and productivity, calling it a paradox, or speculating about unproductive lag times, as technological innovations slowly supplant their predecessors.

Let me tell you where I come down on this: I believe firmly that in each of the sectors you and I represent, gains in productivity and value have been fundamentally driven by advances in information and communication technology.

I have seen countless examples of this over and over again in cities and countries around the world.

Substantial improvements in revenue-per-employee are almost always linked to investments in technology.

For us and for our clients, information advantage equals competitive advantage.

It's how we coordinate across borders—among our member firms and clients—and it's how we keep a 150-country network focused on consistent client service.

At an individual-user level, the computing software and hardware gains of just the last few years have truly been extraordinary: today's technologies and tools are savvy, sophisticated and embraced by an ever-more confident population.

And on a more personal note, from my experience on September 11, 2001, I can speak first-hand of what it's like to

try to operate without the advantages of technology and in a virtual IT blackout.

It can't be done. And yet it has to.

As I and 3500 of my colleagues walked away from the World Financial Center on September 11, and as the two towers collapsed, we lost our land lines, we lost our voice mail system, we left behind our laptops as we gave the evacuation order, and our cell phone service was not reliable. I discovered on September 12, I cannot run my business without technology.

As we began the process of trying to account for everyone, the web behaved exactly like it was originally designed, as a backup communication system. My leader of our merger and acquisition practice had supplied Blackberries to all 200 members of his team. So he knew the status and needs of his team within two hours of the tower collapses, while it was almost 48 hours before I had a 100 percent accounting for my other teams.

So here's what keeps me up at night about the Cybersecurity threat: the productivity gains we have enjoyed are at risk until we figure it out and formulate a response.

Because the same technologies and information priorities that create advantages for business and help people fulfill their potential also create potential vulnerabilities.

You know what these are. Cloud computing. Multiple network access points. More powerful applications and computers. An insatiable demand for more and more data, at faster and faster speeds, all delivered 24/7.

And open architectures, which some argue actually reduce security risk in the long run, as more "good guys" can help build, analyze, debug and improve systems - while the contrary viewpoint is that they inherently increase risks.

On the softer side, consider the popular culture realities of information-sharing.

And a younger generation seemingly less inclined than its predecessor to be wary of privacy pitfalls, or mindful of traditional security measures—fostering an uninhibited and borderless cyber culture.

In the business world, on one hand we look at a whole host of "Web 2.0" computing applications and approaches and we think, "This is exciting. This is new."

And we also pick up the paper every day or log on to *The Financial Times* and read about cybercrime that seems directly linked to cracks in the system, personal and social errors in judgment related to web collaboration, or both.

We know we can't build a "Great Wall" to enclose our electronic or virtual communities, because that would surely defeat the purpose of their existence.

And we know we can't bury our head in the sand.

And so, we are at crossroads. Right now. Right here. And we know there's much to do. Together.

I'd like to finish my remarks this morning by suggesting some ways you might look at the work ahead—especially in your sector breakthrough groups.

It is clear to me that the Cybersecurity risk demands a response that is global, integrated and aligned with key stakeholders' interests—including those of the international enterprise.

Ours is an age of global interdependence—economic, environmental and digital.

We have learned that interdependent challenges require a collaborative approach and that private-public partnerships are essential.

This is not a completely new idea—over the centuries, collective personal, corporate and governmental accountability has led to trust, progress and prosperity on land, in the air, at sea and in space.

Now, the 21st century presents a new realm with a new risk: Cyberspace.

I am confident that we will rise to meet this challenge, that we will find the right path forward, and, as a result, that the information- and digital-based gains of the last decades will continue unabated.

It won't happen by magic, but it will happen.

It will happen because organizations around the world are already beginning to understand that the only appropriate response to Cybersecurity threats is a consistent, enterprise risk management approach that systemically integrates a cyber mindset and addresses cyber realities.

Global enterprise and its leaders will do their part: acknowledging the challenge and addressing it as a key business priority.

It will happen, because I know I cannot look at Cybersecurity risk as something that I can "outsource" to my CIO or my Global Security Officer. That I can't consider a safe and secure international network an "entitlement." And that at Deloitte, the responsibility and accountability for addressing the risk belongs to every one of our organization's 170,000 professionals and to me as a business leader.

And it will happen because you will help frame the risk and shape the response. Because you know exactly what is at stake. For worse, or, I hope, for better.

Together we will find the right, solutions-based response.

We will agree on standards and accountability—not just best practices—and we will secure commitments from organizations to get their own houses in order, with plans that are ongoing, measurable and sustained.

We will understand that a "fortress and wall" approach to the threat of Cybersecurity risks is not enough and that we must re-define not only what it means to be risk-aware, but what it means to be risk-intelligent.

And, ultimately, it will happen, because we really are all in the same boat.

And working together, we can and will identify the dangerous waters, find our common direction, and chart a safe course.

Thank you very much, and I wish you all best for the remainder of the Summit.