



The Global Enterprise Role in Cyber Security

2010 Workshop on Cyber Security and Global Affairs

Adel Melek
Global Leader, Information & Technology Risk
Deloitte Touche Tohmatsu

Zurich, Switzerland
July 8, 2010

I can't begin to express what an honor and a pleasure it is to be here at the Workshop on Cyber Security and Global Affairs. Looking around the room, talking with many of you earlier, and listening in on the sessions, I can't help but be optimistic that the vexing problems of cyber security can be successfully addressed.

But my optimism is firmly grounded in the realities of the challenge. We face a difficult task that will require us to be persuasive, resourceful, and determined. It will take plenty of money and an even greater amount of talent. It will involve the close collaboration of the public, private, and NGO sectors.

But it starts with us, the likeminded individuals who have gathered for this conference. By harnessing our collective brainpower and dedication, by working cooperatively and collaboratively, we will succeed.



Sometimes when I listen to presentations that are given to less technically-inclined audiences, the speaker will trot out the horror stories. They fill their Powerpoint decks with news clippings of the latest security and privacy breaches. They raise the specter of power grid takedowns, air traffic disruptions, government shutdowns, and e-commerce denial-of-service attacks.

I understand the approach, but I think it can be counterproductive, so I've been trying to steer my talks away from sensationalism to focus more on the objective facts.

Of course, here at this conference, the magnitude of the cyber-security problem is fully appreciated. No scare tactics required.

In fact, the challenge that we face is not in convincing ourselves, but in persuading others. Outside these walls is an environment of misunderstanding, of secrecy, of complacency, and inertia. These are the enemies that we face, and they are every bit as real and as dangerous as hackers, rouge governments, and cyber-terrorists.

As you are well aware, public attention spans are short. The media is fickle. Today's hot story is tomorrow's forgotten trivia.

When millions of credit card numbers are stolen, interest spikes, but it just as quickly wanes. So our challenge is this: How do we convince business leaders, government officials, and the public that even though the story has faded from view, the problem hasn't gone away? How do we make them realize that while public focus has turned elsewhere, the bad guys are still working relentlessly to gain the upper hand?

Over the next few minutes, I will offer some ideas on how we can break through this complacency. But here's a key point that we would all do well to remember: cyber security is not solely a technology issue. In fact, I would argue that it is not even primarily a tech issue. Rather, it is a risk management issue. It is a public relations issue. And it is a people issue. And any solution we come up with will need to acknowledge and accommodate these realities.



One way to break through the logjam of complacency is to put the problem into understandable terms. The analogy I have been favoring of late has a military basis: cyber security as war.

Now some might say that a war analogy is melodramatic and sensationalistic. My response is that, if anything, it understates the threat. Consider some of these facts:

- As of right now, at least 20 countries are engaged in a cyber arms race, building capabilities, conducting R&D, and training their people for cyber warfare.ⁱ
- At least five countries -- the United States, China, Russia, Israel, and France -- now have offensive cyber capabilities to infiltrate systems, disrupt networks, and take out strategic targets.ⁱⁱ
- In a recent survey, 60 percent of IT security executives said they believe that foreign governments are involved in infrastructure infiltrations.ⁱⁱⁱ
- Cyber security attacks cost \$6.3 million a day worldwide.^{iv}
- In 2008, the global costs associated with stolen data was estimated at \$1 trillion dollars -- and that figure is probably low by an order of magnitude.^v

When you lay these facts out, perhaps a war analogy is not that far-fetched.

Another reason I use the cyber-security-as-war analogy is that it puts the issue into terms that non-technical people can understand. The whole cyber-threat problem can be abstract and complex and thus difficult to fully grasp. Anything we can do to cast the issue in more familiar terms will help the cause. We need to move away from the perception that cyber-security is primarily a geeky, technical concern and move toward the idea that the problem affects -- and the solution involves -- everyone.



Once we have framed the *problem* using war terminology, it makes logical sense to put the *solution* into similar terms as well. And, fortunately, our analogy holds up nicely in this regard.

When we think about war, especially when we think about those wars that had successful outcomes -- wars that the good guys won -- we can find a thread of commonality. That thread is strategic alliances.

Consider how vastly different the outcomes of World War I and World War II would have been, were it not for the allied forces combining to achieve victory.

Think of restoring order in Kosovo, which was accomplished by an international team of peace-keepers.

Consider the role that international pressure played in ending apartheid in South Africa.

Even within the last year, we have an example of the power of strategic alliances -- the case of pirates off the coast of Somalia. These terrorists of the high seas had set up shop in a lucrative spot -- more than 10 percent of the world's ocean-going trade passes by the horn of Africa. And the pirates were earning handsome returns on their efforts -- one calculation I saw put the figure at \$150 million in paid ransoms^{vi}. The attacks were getting more brazen and more frequent until the problem could not be ignored any longer. Finally, the international community took action, and, in a coordinated effort, sent warships to patrol the area and confront the pirates. More than 20 nations took part in the effort at a collective cost in the hundreds of millions^{vii}. As a result of this international cooperation, piracy incidents plummeted and the seas around the horn of Africa became significantly safer for sea trade.

Of course, war and piracy are not the only areas where coordinated responses yield positive outcomes. For example, think of Lyndon Johnson's "War on Poverty" in the 1960s. He used a war analogy to emphasize the seriousness of the issue, and to galvanize and inspire the public.

President Carter used the analogy with less success in the 70s. During that decade's energy crisis, he called the quest for energy independence the, quote, "moral equivalent of war," end quote. What undermined his crusade, unfortunately, was the fact that the acronym for "moral equivalent of war" is "meow."

Do you remember the ozone hole threat? You can be forgiven if you don't, since the issue peaked in the public consciousness over two decades ago. One of the reasons you don't hear about the ozone hole anymore is because the problem was solved. And, to my point, it was solved through an international effort. In 1989, the Montreal Protocol -- which was ratified by 196 countries -- went into effect, banning the production of ozone-depleting chemicals. Due to this agreement, the ozone layer is projected to fully recover by the year 2050. The former secretary-general of the United Nations, Kofi Annan, characterized the Montreal Protocol as, quote, "perhaps the single most successful international agreement to date," end quote.

Do you remember the Y2K threat? Hopefully, more people will recall this one. Chaos was predicted to ensue when computer clocks rolled over from New Year's Eve 1999 to New Year's Day 2000. The fact that problems were limited and isolated is interpreted by many as evidence that the massive reprogramming effort that took place in the years prior to the millennium was successful.

Among the steps taken to solve that problem was the formation of the International Y2K Cooperation Center, which promoted national readiness, global cooperation, facilitation and assistance.

Other current issues provide examples of international cooperation, including climate change, AIDS, flu pandemics, and other health issues.

We should be instructed and inspired by each of these examples. They clearly demonstrate not only *what* is possible, but *how* it is possible. The cyber-security problem cannot be solved in isolation, any more than the British, on their own, could have won World War II; or Brazil, to choose a random country, could have fixed the ozone hole by themselves.

There are more parallels to war that can be instructive. For example, just like in war, our response cannot be only defensive. We need intelligence and deterrence as well as offensive and invasive capabilities.

It's also generally true that for wars to be successful, you need a charismatic leader who galvanizes his nation behind him. Think Winston Churchill and Franklin Delano Roosevelt. This is actually a major need area for the cybersecurity movement -- the absence of a global influential leader. We need a crusader, someone with unimpeachable integrity and high qualifications to lead the charge. Who might it be?

I should point out the limits to my war analogy. The battle for cyber-security is not similar to a traditional nation-state war, with soldiers and tanks and arms. Rather, it is more like a guerilla war or terror war, with an elusive enemy, who may not be tied to any particular nation, and who may even be acting as an army of one.

In this war, we will not have a moment of decisive victory or defeat. Rather, we will have a never-ending series of skirmishes. In this effort we must be ever-vigilant. It is truly a war with no end.



Before I delve too deeply into additional ways that we might approach the battle for cyber-security, I'd like to outline what I see as the major problems that must be addressed.

One of the biggest challenges is the sheer **ubiquity of technology**. From the smart phone in your pocket to the GPS satellite that your phone is perhaps talking to right now, we are awash in digital devices.

There is not a major industry in the world that could keep operating in the face of an IT infrastructure shutdown. Travel, finance, healthcare, retail, energy -- all have made huge advances thanks to technology, and all are dangerously vulnerable thanks to that same technology.

The threat includes even the military, with its drones, its simulated war games, and its high-tech weaponry. The military/technology link is an especially vexing issue for smaller countries, which may lack the sophistication and resources to compete and defend itself in a cyber world.



Another problem we face is the **patchwork of laws and regulations** around cyber-security. Not only do we lack harmonized global regulations -- we don't even have agreement on the need or a shared understanding of what such regulations might look like.

So maybe a *global* regulatory solution is too ambitious. Perhaps a *regional* solution would be more attainable. Unfortunately, we fall short here as well. For example, within the EU, there's no comprehensive cyber-security strategy. In fact, there's not even a shared standard for personal privacy laws between EU nations^{viii}.

Okay, so maybe we need an even smaller, more manageable group. Maybe something like the G-8. Unfortunately, once again, we find a void. Within the G-8, there is little evidence of coordination around cyber-security issues.

Setting our sights even lower, we turn to a *single* jurisdiction. Surely, one country can have its security and privacy regulations sorted out. Well, if that country is, for example, the United States, the answer is no. What you find is 50 states and almost as many regulations.

This regulatory patchwork inhibits commerce. Just look at the faltering steps of YouTube and Facebook as they try to gain a toehold in Europe. Or look at Google's struggles in China, and you can see the negative impact of a lack of regulatory harmony.

Unfortunately, sometimes new regulations can be worse than no regulations at all. In most instances, the new laws will lag so far behind technological advances that the damage is already done, and the law is irrelevant or ineffectual.

In other cases, new regulations may mimic the threat of the physical world rather than the realities of the digital world. For example, if someone breaks into your house and steals your flat-screen TV, you know it -- the door is kicked in and the TV is gone. In the cyber world, the stolen item is not even missing; the personally identifiable information or the intellectual property is right where you left it, seemingly undisturbed. Victims often have no clue that they've been robbed.

We are limited in this area by time and experience. We have had centuries of experience in the physical world that allowed us to develop our laws, regulations, perceptions, behaviors, and cultures. But in the case of the cyberworld, we have seen a tremendous evolution in a short period of time -- two decades at

best. As a result, we lack the precedence, the history, and the data. There is no transparency associated with breaches. There are very few laws that force organizations to report them, and as such, we are less convincing in our arguments and in elevating the threat to its rightful level.



Another problem arises with **emerging technologies**. It's no longer enough to keep up with the *black hats* as they create havoc and exploit vulnerabilities. Today, we must also cope with the *white hats* in R&D labs, in universities, and at start-up companies. As new technologies emerge, they create advantages for business and help people fulfill their potential, as intended. But at the same time, they create vulnerabilities that must be assessed and addressed.

For every advantage gained — from cloud computing, multiple network access points, open architectures, and mobile devices — new risks emerge. Sometimes, in the rush to market, shortcuts around security are taken, with fixes only introduced in the second or third generation. The first iPhone, for example, was rejected by many corporate IT departments due to its security vulnerabilities. Only with the second and third generation have these phones been able to make significant gains in business market share.

And, of course, we all know that the pace of development will never slow. Depending on your perspective, this relentless innovation is either the genie's bottle or Pandora's box. Either way, it's open and there's no closing it. Today, even appliances and cars are starting to sport IP addresses. Tomorrow, clothing and implantables may be the new cyber frontiers.

And maybe when a cyber-terrorist hacks into the chip implanted in your brain, we will all finally agree that we've got a problem.



Our list of issues to address also includes what I call "softer" risks -- the risks associated with our **culture**, with human behavior, and with value systems.

We have seen in just a few short years the rise of the networked generation. Young people today use texting as a primary means of communication. They post all sorts of intimate information on Facebook. They think nothing of having their whereabouts continually tracked by GPS; they casually post their full birth date along with other identifiable information online. They are less wary of privacy pitfalls, and less mindful of security measures. They live in an uninhibited and borderless cyber culture.

The digital generation is comfortable with technology and using it has become second nature. But they tend to focus on the benefits and look right past the risks.

Another challenge we deal with is the lack of transparency and informed reporting associated with cyber security threats, incidents, and their true impact. When President Obama recently cited the estimated loss of IP to be approximately \$1 trillion dollars, I remember being interviewed by a business network TV station. The reporter asked me whether he heard right or was it a billion dollars? Many business leaders don't seem to relate to the true number and don't understand the magnitude of the issue until something happens in their own organization, or to a peer who was unfortunate enough that the incident became public knowledge.

Another example comes from the financial sector. Many financial services companies make a point of keeping the customer "whole" in the event of a security breach. This approach clearly benefits the customer and helps maintain the reputation and trust of the financial institution. But at the same time, it

leads federal prosecutors to call these situations a “victimless crime,” which of course it is anything but. And thus we let the problem perpetuate.

This presents a challenge for us, because the future of cyber-security lies in cultural competency. To successfully address the threats, awareness must be raised and behavior must be shaped -- especially among the generation that is coming of age.

Cultural competency also comes into play on the organizational level. It encompasses familiar HR mantras like leadership, change management, tone at the top, and role modeling. It has a strong educational component. It involves governance and information management.



In dealing with cultural issues, we also must face up to the **perception** problem. If the public doesn't grasp the nature or magnitude of cyber-security, perhaps the problem is with us, not with them. We need to do a better job of expressing ourselves, of clearly explaining the issues.

In this area, we'd do well to rip a page from the political playbook. We need to emulate the savvy politicians who have mastered the art of framing the issues.

For example, if a politician believes in limited government, you will surely hear him or her talking about tax “burdens,” not tax “revenue.”

If they are beholden to big oil, they will freely talk about “energy exploration” but will never talk about “oil drilling.”

And you have undoubtedly noticed that the “global warming” debate has been reframed. Now we talk about “climate change.”

These subtleties of language are actually powerful tools for motivating and changing behavior. We need to *frame* the issue in order to *solve* the issue.

To do so in the realm of cyber-security, we need to talk more about “risk” and less about “security.” “Security” to many people means locking resources down. The problem is that electronic information has no value if it doesn't move.

If we talk about the problem in terms of risk, we are reframing the issue in a manner that will enhance understanding. The word risk defines the threat as a constant issue that demands ongoing attention. It implies that every day we'll face another battle to be won or lost.



The last problem area I'd like to address concerns **talent**. Our adversaries are intelligent, resourceful, and motivated. The only way an enemy like that can be subdued is by deploying our own allied army of similarly endowed cyber warriors.

Unfortunately, right now that army is not in the best of shape. They are poorly trained and inadequately equipped to handle the task at hand. They run the risk of being outgunned and overrun on the battlefield. It is not unlike the adjustments needed to prepare a conventional army to fight terrorists and guerrilla armies.

According to a recent security survey by the SANS Institute, 90 percent of respondents are having difficulty recruiting qualified cyber-security workers. They reported staffing problems in the areas of strategy, policy guidance, risk management, incident response, and threat management^{ix}.

Clearly, we need to re-arm our cyber army. A number of countries are taking steps to fill the talent gap. In the United States, two federal security agencies jointly sponsor the National Centers of Academic Excellence programs. The goal of these programs is to reduce cyber vulnerability by promoting higher education and research.

Meanwhile, in the UK, public competitions are being held to find talented recruits. A program called the Cyber Security Challenge tests the IT skills of participants to identify future cyber security professionals. Top performers in the competition are awarded prizes including scholarships, training courses, and mentoring. This collaborative program is backed by UK commercial, academic, and public sector organizations^x.

The UK has also created a Cyber Security Operations Centre that provides education and advice to businesses around cyber threats.

China develops much of its cyber security talent through military channels. The country has established several training centers that provide cyber war training programs to military recruits.

These programs are limited, but they are a start. More must be done. And resources are available to get it done. At Deloitte¹, we advise our clients to apply for grants from governments, NGOs, and private foundations to help develop their technical talent. This money is available and should be tapped. Every grant awarded and every person trained will make a difference in this battle.



Okay, that covers some of the major challenges we are facing. Now, the big question: what to do about it?

I already touched upon what I consider the key -- strategic alliances and collaboration. The problem is too big for an individual person, organization, or even country to grapple with. We are facing a borderless problem for which there must be a borderless solution.

We need to bring governments, businesses, NGOs, and academia together. We need to enhance the *ability* -- and perhaps more important, the *legality* -- of these entities to share information.

I realize that privacy and civil rights activists shudder at the notion of anything that might undermine personal liberty and the right to privacy. I share this concern. I am a firm believer in individual freedom.

Yet in advocating for freedom, a balance must always be attained. Society has decided, for example, that my freedom to drive 200 kilometers an hour is overruled by society's need for safe streets. And my freedom to smoke is superseded by my fellow citizens' right to breathe smoke-free air.

Similar safeguards can be employed in the cyber realm. As we work to flush out those who pose a threat to IT infrastructure, we must ensure that innocent bystanders don't get caught in the crossfire.



In terms of promoting strategic alliances and collaboration, recent activity is encouraging. This conference alone gives us cause for optimism. This year's event is the second annual Workshop on Cyber Security. I

hope to attend many more of these conferences in the future, as they help us develop a coordinated response to the challenges we face.

Other events help create and sustain momentum. For example, a few months ago, the International Forum on Cyber Crime took place in France, attended by 1,500 cyber-security experts from 23 countries.

The Worldwide Cybersecurity Summit took place in Texas in May. And we've got the International Conference on Cyber Security coming up in New York next month.

Beyond conferences, countries are also taking the threats more seriously. We've recently seen the creation of centralized agencies dedicated to cyber security in Singapore, South Korea, Australia, Malaysia, Japan, and Hong Kong.

At my own organization, Deloitte, we recently opened the Deloitte Center for Cyber Innovation, as well as the Deloitte Center for Security & Privacy Solutions. These centers serve as information clearinghouses; they conduct research and surveys; they develop tools and methodologies; they offer education and training.

These are all fronts in the battle to subdue our common enemy. Moving forward, we should strive to strengthen the ties between these independent and sometimes isolated initiatives. Collaboration will be key to our success.

Another critical success factor will be the role of government. While the government neither can nor should solve the problem on its own, it has a vital role to play in the areas of regulation and incentives.

Regarding the former, I realize that regulation can be a polarizing topic. Many businesspeople bristle at regulatory constraints, claiming that they stifle innovation, sap resources, and cost millions. On the other hand, proponents claim that regulation is needed to curtail excessive risk-taking and to smooth the rough edges of capitalism.

As is often the case, the arguments on both sides have merit. We have all recently witnessed the effects of a regulation-free business environment. At the same time, many of us are aware of the burdens imposed by excess regulation.

In terms of cyber security, I believe that carefully constructed, globally-adopted regulations can be of great benefit. These should be "rules of the road" -- analogous to those regulations that govern other forms of commerce such as air travel or container shipping. The key will be finding the proper balance between inducing the right behavior and inviting negative effects of over-regulation.

One regulatory area worth exploring is the creation of reliable standards and metrics for cyber security. Private operators, such as ISPs, equipment manufacturers, and software developers, can then use these metrics to establish competitive advantage. These adopters can earn tax breaks, gain preferred access to government contracts, and qualify for other performance-based rewards.

Governments can also assume a gatekeeper role by making access to a nation's economy contingent upon adherence to cyber-security standards and protocols. This would not be a radical or unprecedented step; governments already do this in many other areas. For example, most governments don't allow the importation of tainted meat. They limit the travel of people harboring infectious diseases. They restrict the distribution of untested pharmaceuticals.

It's time to add cyber-security to this list.

As I noted earlier, government can't do it alone. Business will play an essential part. The rationale for the deep involvement of business is strong, and, indeed, a case can be made for why business should lead the way.

In meetings with clients, business leaders sometimes ask me why they should care. Why are cyber-security risks relevant to their business?

These questions reflect a lack of understanding among many business executives of the risk, its magnitude, impact, and relevance. Once executives understand these three issues -- the threat; the probability of it happening to their business; and the eventual impact on their reputation, trust, and finances -- they tend to make the right decisions, develop the right policies, and dedicate the necessary resources

When speaking to my clients, I say that cyber-security is important because your company isn't actually in the financial services business (or the healthcare business, or retail, or whatever it may be). What you are really in is the information business.

After that sinks in for a minute, I tell the executive that information is the de facto global currency; that the flow of goods and services is inextricably tied to the flow of information about those goods and services.

If the executive is still dubious, I ask, "Where would Fedex be without tracking data? Where would Vodaphone be without cellphone user data? Where would Wal-Mart be if they didn't have inventory and supply chain and transaction processing data?"

And this revelation usually makes true believers of businesspeople. I say that despite whatever business you think you are in, you are really in two businesses: The one it says on your business card, and the information business.

Once that issue is settled, I probe a little deeper on the "why should I care?" question. I point out that private industry has a huge investment in, ownership of, and responsibility for the IT infrastructure around the world. In the United States, for example, industry owns somewhere between 85 and 90 percent of the critical telecom-datacom infrastructure, including almost all of the wireless infrastructure^{xi}.

In other nations where technology penetration is highest, the percentage of privately owned or public/private partnership-owned infrastructure is also high.

Even in instances where the government owns or controls most of the infrastructure assets, private industry has intersecting interests in terms of licensing, e-commerce, research, manufacturing, and investments.

Given these compelling reasons to care, one might expect the international business community to be proactive about cyber-security risk. Unfortunately, that's not always the case.

The global business community *does* agree, in general, about the need for a deeper understanding and more education around cyber-security issues. But this broad agreement hasn't prevented business from lagging other sectors in its readiness. By many measures, the military and political sectors are more advanced than business in terms of effectively addressing cyber concerns. And there's little doubt that hackers, cyber terrorists, and rogue governments have more advanced capabilities than many in the private sector.

This perception that business is lagging was validated in Deloitte's 2009 Global Security Survey of the technology, media, and telecommunications industry. The survey reported that a full 60 percent of IT leaders said they are "falling behind," or still "catching up" to known security threats^{xii}.

The historical trend is not positive in this area. Only 49 percent of respondents felt this way in a survey conducted just one year earlier^{xiii}.

Another recent survey also documents the runner-up position of business and industry. The 2010 CSO CyberSecurity Watch Survey concludes that cyber crime is a more common and larger threat than is generally realized. It also notes that criminal innovation and techniques have outpaced traditional and current security models and detection technologies^{xiv}.

All of which begs the question: Why is the international business community lagging in cyber-security?

I think a number of factors come into play. For one thing, the cyber-security threat is a relatively new risk classification, one that is growing and changing quickly. The threat is analogous to cancer: it can spread dangerously; and it requires aggressive and sometimes continual treatment.

However, unlike a disease, we don't have comprehensive assessments and diagnoses. We don't have precise definitions and nomenclature. And we don't have clear cures, processes and proven success stories.

We need all of these things if we are to help the patient. Which puts all of us in this room into the roles of doctors and medical researchers. Our diagnoses must be clear and accurate and free of jargon that will only confuse the patient. Our definitions and terminology and metrics must be harmonized so that we have a basis for discussion and comparison. And our processes and tools must be well-thought out and effective. The health of our IT infrastructure depends on us getting this right.



This conference, and others like it, will only be considered a success if it spurs action and progress. We can talk all day, and we can congratulate ourselves all night on our insights and our understanding of the threat. But if we can't translate all this into genuine action that moves us forward, then we have all just wasted each other's time.

In the spirit of progress, I'd like to put forth a few suggestions. Please take one or two of them to heart and act upon them.

My **number one** recommendation is to **get active**. Take on leadership roles in security and privacy organizations. Head up a task force. Reach out to your peers. Share best practices.

Two, evangelize. Do whatever you can to increase public/private collaboration. Inform your executives, and boards. Contact your legislators. Write opinion essays. Give speeches. Sit on panels. Become a "go-to" person for the media.

Three, stay positive. We need to be continually vigilant about the threats that make cyber-security necessary, but we shouldn't lose sight of all the positives that good cyber-security can enable.

Four, try to change attitudes. Our colleagues in the public and private sectors need to approach cyber-security as the ongoing management of a continuous risk, not as a tactic for stopping a specific future attack.

Five, broaden the discussion. Fight the misconception that cyber-security is solely a technology issue. Promote the need for cultural understanding and a willingness to practice secure behaviors.

Six, dispel misconceptions. Many people still refer to cybersecurity as an “art” not a “science.” We need to dispel this notion and get over it. Art is unique, not reproducible, not describable, and may not even be appreciated by everyone. Science, on the other hand, is something you can document, reproduce with accurate results, describe, and measure. We need to encourage the idea that we are working in the realm of science, not art.

And seven, prioritize. Identify key assets and likely threats, then focus security resources accordingly. If you call everything critical, nothing actually is.

The world has entered an unprecedented era of interdependency. It's true in the environmental realm, where a volcano in Iceland wreaks havoc with travel across Europe. We've seen it in the economic realm, where a banking failure in one country can wipe out pensions in another. We've seen it in industry, where a safety recall in the U.S. undercuts market capitalization in Japan. We've seen it in the social-political realm, when a terror attack in one country send shudders across the world.

All of which emphasizes my main point. We have created an interdependent IT infrastructure, and now we have to live with that reality. Cyber-security is a global issue that requires a global response. The problem is transnational, people-driven, and integrated into almost every aspect of public and private life. Any solution needs to address those realities.

Right now, our approach is immature and often ineffectual. We need to quickly move from the *reactionary* to the *proactive* to the *preemptive*. The use and dependability of cyber networks is critical to our economic well-being, and resources must be devoted that are commensurate with that fact.

When you consider that we have early warning systems in place for things like the weather, earthquakes, nuclear war, and runs on the stock market, it boggles the mind that we haven't created similar systems around cyber security.

There's plenty of historical precedent for getting it done. Over many centuries, our collective personal, corporate, and governmental accountability has led to trust, progress, and prosperity on land, in the air, at sea, and in outer space. We need the same constructs for cyber security.

In my view, and the view of many of my colleagues at Deloitte, there's really only one appropriate response to cyber-security threats -- a consistent, risk-intelligent approach that systematically integrates a cyber mindset and systematically addresses cyber realities.

As a group, we collectively need to do our part by helping to frame the risk, to shape the response, and to agree on standards and accountability. We need to redefine not only what it means to be risk-aware, but what it means to be risk-intelligent.

At the start of my remarks, I said that I don't need to convince anyone in this room, and, of course, that's true. The magnitude of the cyber-security problem is fully appreciated here.

So let's leverage our shared perspective. Let's continue to evangelize, to promote, to talk up the issue. Let's collaborate, coordinate, and communicate. We don't need scare tactics or overblown threats -- the real world is scary enough and the media reports on it daily.

Rather than focus on the imminent threats, let's focus on the solutions and the good things that can come from enhancing our mutual cyber security.

We will never eliminate the threat. Our vigilance must be constant. But we can control the threat. And we can collectively prosper.

Let's go forth and do just that.

Thank you.

Endnotes

ⁱ Neo, H. M. (2010, January 28). China, US, Russia in cyber arms race: net security chief. Retrieved June 10, 2010, from Google News: <http://www.google.com/hostednews/afp/article/ALeqM5gBI-UmsuwvR6i-mxI5TDGvDuGtrw>

ⁱⁱ Ibid

ⁱⁱⁱ Ibid

^{iv} Ibid

^v Mills, Elinor. "Study: Cybercrime cost firms \$1 trillion globally." CNET News. 28 Jan. 2009. 12 Apr. 2009 <<http://news.cnet.com>>.

^{vi} "Pirates 'gained \$150m this year'" BBC News. 21 Nov. 2008. 12 Apr. 2009 <<http://news.bbc.co.uk>>.

^{vii} Knott, John. "United Kingdom: Somalia: Clan Rivalry, Military Conflict, And The Financial And Human Cost Of Piracy." Mondaq. 17 Mar. 2009. 12 Apr. 2009 <<http://www.mondaq.com>>.

^{viii} Mann, J. (2010, March 31). Europe Declares War on Cyber Crime. Retrieved June 10, 2010, from The New New Internet: <http://www.thenewnewinternet.com/2010/03/31/europe-declares-war-on-cyber-crime/>

^{ix} Ashford, W. (2010, April 27). UK Cyber Security Challenge to find next generation of security experts. Retrieved June 10, 2010, from Computer Weekly: <http://www.computerweekly.com/Articles/2010/04/27/241057/UK-Cyber-Security-Challenge-to-find-next-generation-of-security.htm>

^x UK launches competition to find cyber security experts. (2010, April 27). Retrieved June 10, 2010, from BBC News: <http://news.bbc.co.uk/2/hi/technology/8645041.stm>

^{xi} "Critical Partnering - The Global Enterprise Role in Cybersecurity," transcript of remarks by James H. Quigley, Chief Executive Officer, Deloitte Touche Tohmatsu, at the EastWest Institute First Worldwide Cybersecurity Summit, Dallas, Texas, May 4, 2010.

^{xii} Ibid

^{xiii} Ibid

^{xiv} Ibid

¹Deloitte as referred to in this newsletter refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms