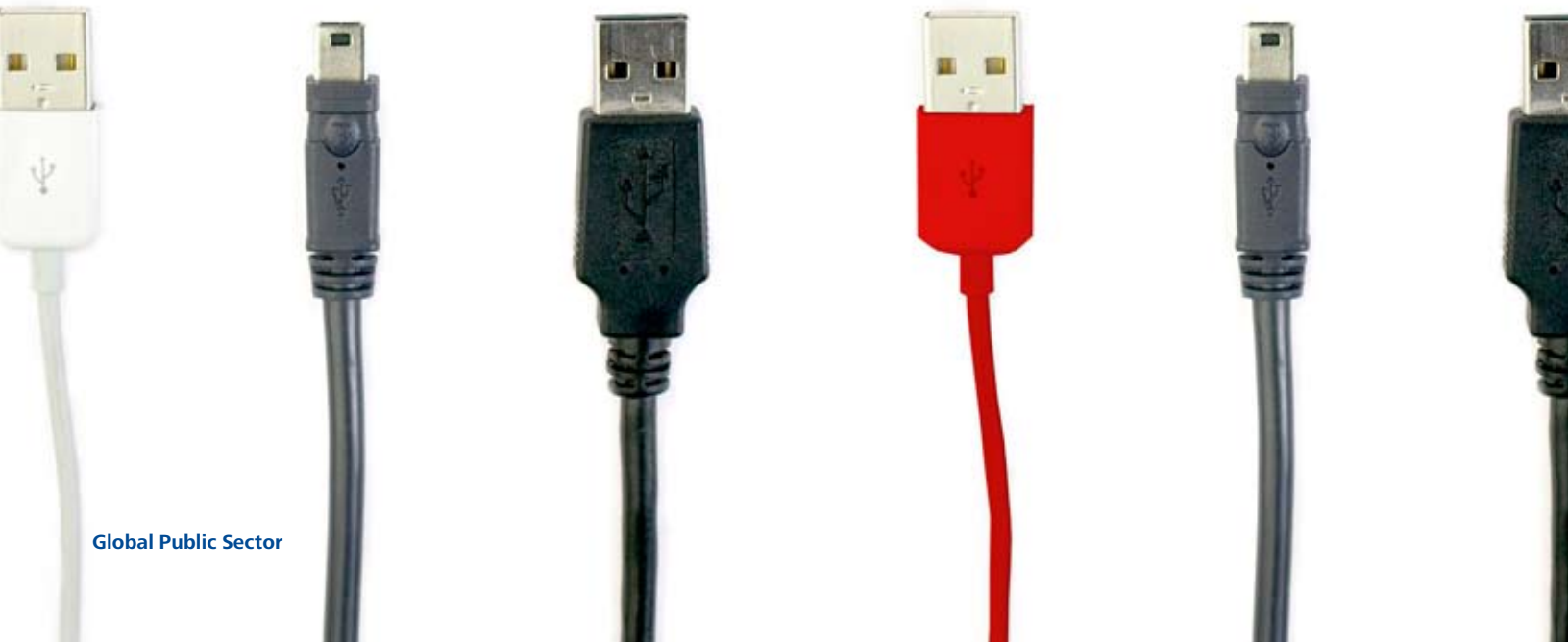
Deloitte.

Cybersecurity: Everybody's Imperative

Protecting our economies, governments, and citizens

With interviews from Deloitte member firm cybersecurity leading professionals from around the world



Global Public Sector

Cybersecurity: Everybody's Imperative
Protecting our economies, governments, and citizens

By

Greg Pellegrino,
Deloitte Touche Tohmatsu Public Sector Industry Leader

and

Gary McAlum,
Senior Manager, Security & Privacy Services, Deloitte & Touche, LLP,
and Colonel (US Air Force Retired)

6 May 2009

Governments around the world need to address cybersecurity urgently so organizations can survive, thrive, and enable economic growth. Cyberspace, which began as an electronic adjunct to other domains such as commerce, today is a domain unto itself, and organizations of all types must be able to function effectively in cyberspace in order to survive.

Cyber culture is growing faster than cybersecurity, so everything that depends on cyberspace is at risk.

The problem is that cyber culture is growing faster than cybersecurity, so everything that depends on cyberspace is at risk. Private data, intellectual property, infrastructure and even military and national security can be compromised by deliberate attacks, inadvertent security lapses, and the inherent vulnerabilities of the Internet. On top of this, the current global economic crisis is amplifying these threats. Governments need to partner with the private sector, citizens, and other governments to work on a holistic, transnational solution that goes beyond technology to combat these threats and enable global commerce, greater transparency in government, and improved data protection. The stakes are high but the risks are even higher: isolation, cyber protectionism, and an inadequate balance between security and civil liberties.

The solution: We must address cybersecurity and the changes in habits and lifestyle that go with it, because there's no way back.

The status quo: Cyberculture is growing and won't stop

Today, access to information is ubiquitous; new business and government activities rely on digital connectivity; and even traditional elements of life like appliances and cars may soon sport IP addresses. Dependence on the cyber domain is no longer limited to advanced technologies, and participation in it is no longer a choice.

The lack of effective cybersecurity threatens not only the gains made possible by information technology, but other elements of life that are now under Internet control. Much energy has been focused on the economic, government and social advantages that a digital world can enable. Now, we must refine the focus – on what a secure digital world can enable. Because an unsecured Internet is worse than none at all.

Twenty years ago no one would have imagined that hackers could use inexpensive, store-bought equipment to shut down governments in other nations. That one espionage operation could compromise information security in more than 100 nations without sending a single agent abroad.[1] Or that a network installation contract could put the entire British communications infrastructure at the potential mercy of a foreign power.[2] Yet these have been actual headlines in the last year, and similar news seems to arrive almost every day. Clearly, the existing system – trusting the creators of cyber resources to ensure their security – isn't working.

Every time technology creates a new domain of dependency, the new benefits come with new risks. We tend to build things for the benefits they promise,

and grapple later with the harms that arise alongside them. Whether in international domains such as aviation, telecommunications, finance and shipping, or through investments in domestic needs such as electric power grid and the highway and workplace safety, governments eventually find mechanisms to balance the risks with the rewards and ensure reliable operation.

The cyber culture is at a perilous midpoint along this traditional sequence of events: The dependency is there, but the security has yet to catch up. Because the global nature of the threat demands uniform standards of protection around the world, it matters little if an individual nation or alliance has advanced its cybersecurity ahead of the rest. Formal, intensive efforts in nations such as the United States, Canada, the United Kingdom, Singapore, Israel and others will make a difference, but as long as data can flow unchecked to and from other states with little or no cybersecurity, the entire global system remains on a collision course with threats of its own making.

Of course, shutting down the Internet isn't an option. Nor is it appropriate to section it off with impenetrable walls that guard against catastrophic future attacks. Information that flows at net speed must continue to flow, threats will arise every day, and those who use it successfully will learn to treat cybersecurity as an exercise in ongoing risk management.

Advice on the many elements of cybersecurity is easy to come by. But putting the pieces together requires a master vision that goes beyond technology and process. The problem is transnational, people-driven, and integrated into almost every aspect of public and private life. The solution should meet those descriptions as well. Because the physical infrastructure that powers the Internet is largely in private-sector hands, government and business must find compatible roles in managing this new culture of risk.

If government can lead people to meet this challenge, the outcome won't be just a set of technological safeguards. It will be a new cultural approach, led by people who "speak" cybersecurity and populated by millions who understand and accept the necessary tradeoffs. The reward will be a society governed by a cyber mindset and enabled to do more than ever with information technology.

What can effective cybersecurity make possible?

Threats of damage, disclosure or loss are foremost when the subject of cybersecurity comes up. Those threats demand to be taken seriously. But a holistic view of the subject also includes positives – the benefits that a more secure global information culture will make available to people and governments.

Taken broadly, cybersecurity can enable greater transparency in government operations. It can increase the efficiency with which government interacts with business, and – through regulations to bolster data protection – it can enhance trust in online business dealings. Government-led cybersecurity can also take a leading role in fostering cultural change, so that people in all walks of life understand the threats and embrace the new measures necessary to preserve security in everyday work and transactions.

A significant beneficiary of improved cybersecurity could be the practice of online government. Interaction between governments and people often involves sensitive information such as tax data or intellectual property included in patent filings. In some parts of the world, people trust their governments with this information – but not mobile applications, or even the Internet itself. In other

places, the governments themselves are held suspect, and cybersecurity can enable a degree of transparency that will increase the public's confidence in its leaders.

Consider what a reliably secure Internet, safe to use from both wired and mobile touch points, can do in both situations: bolster trust and speed the process of government itself. When we speak of cybersecurity as an investment, not merely a cost, this is the payoff.

The same advances, of course, can offer similar benefits to the private sector. Wherever lack of trust in the Internet stands as a barrier to greater, faster, more widespread commerce, cybersecurity has the potential to unlock those transactions and speed the economy of any jurisdiction that makes the investment. A secure Web means efficiency, and efficiency is an ingredient of prosperity.

The other side of the coin? Potential isolation. When enough governments establish the cyber-secure conditions described above, people the world over will come to expect those safeguards. Where the safeguards aren't in place, people and governments may find themselves shut out from participation in the new economy.

The other side of the cybersecurity coin? Potential isolation.

There is also the potential for political leaders to display cultural leadership. The digital generation is intimate with the use and power of the Web, but may tend to focus on the benefits and look past the risks. The analog generation is comfortable with the daily need to manage risk and protect assets, but may come to the Web less naturally. If leaders set the example for a culture of cybersecurity, the result could be that members of both generational groups will be attuned to the special nature of risk on the Internet. People would be more likely not only to police themselves, but also to recognize misuse by others and flag it for corrective action.

At a glance: How governments should approach cybersecurity

- Be vigilant about the threats that make cybersecurity necessary – but don't lose sight of the positives that good cybersecurity can enable.
- Identify and catalog critical infrastructures that are vulnerable to cyber compromises.
- Approach cybersecurity as the ongoing management of a continuous risk, not as a safeguard against specific future attacks.
- Don't think of cybersecurity as merely protecting digital assets. The digital domain influences almost every other part of life – so cybersecurity is ultimately about protecting everything of value.
- Remember that cybersecurity cannot be achieved through technology alone. It requires a cultural understanding and a widespread willingness to exhibit secure behaviors.
- Recognize the central role of the private sector in both creating and using cyber assets. Treat cybersecurity as a public-private partnership, not a top-down mandate.
- Plan for resiliency – the ability to react and recover when cybersecurity is compromised despite protective efforts.
- Treat cybersecurity the way you treat customs, food imports and immigration – make access to your market contingent upon adherence to safety standards you determine.
- Identify key assets and likely threats, then focus security resources accordingly. If you call everything critical, nothing actually is.

Businesses and governments have plenty of experience applying the techniques of risk management to financial and material assets. Today's challenge is to adapt those tools to the ongoing protection of cyber assets.

Think "risk" more than "security" – and people more than things

The terms "cybersecurity" and "cyber risk" may be used almost interchangeably. However, each speaks to a different mindset. Security is about locking resources down – keeping them safe in a box. But the information carried over the world's electronic channels has no value if it doesn't move. Defining the problem as "risk" acknowledges that the threats are constant, and that every day brings another battle to win or lose.

Whether or not we are already at cyber war – another distinction that's largely semantic – the military analogy is appropriate. The effort to protect information assets will not have a moment of decisive victory or defeat. Rather, it can be compared to a blockade or the enforcement of a no-fly zone.

Businesses and governments have plenty of experience applying the techniques of risk management to financial and material assets. Today's challenge is to adapt those tools to the ongoing protection of cyber assets. The outcome will be a new paradigm that includes cyber risk as a manageable threat, and cybersecurity as an expertise that people demonstrate every day in their personal and professional lives.

This shift in thinking cannot be accomplished by technological means alone. Hardware and software safeguards will remain important, but the future of cybersecurity lies in cultural competency. When the Deloitte Center for Network Innovation identified the five pillars of what Deloitte professionals call "Netcentricity," only one – communications infrastructure – was purely technological. Organizational governance, information management, and human leadership are pillars of their own.

Call it war or don't, but it's happening now

Another fallacy of the security paradigm, as opposed to the risk paradigm, is to imagine cyber threats as future possibilities – as spectacular failures or attacks that may happen if we don't prevent them.

Such threats do exist, but others are already in play, and a risk-based approach acknowledges this. Right now, cybercrime costs the global private sector as much as $1 trillion in intellectual property each year.[3] A contractual relationship between government and private entities, coupled with use of a peer-to-peer file sharing network and apparent human laxity, recently allowed the blueprints and avionic schematics for the U.S. president's planned replacement helicopter to show up on a computer in Tehran (Iran).[4] And while it may sound melodramatic to say so, these are, after all, only the instances we know about.

Because security compromises are part of the reality governments must deal with, it is important to complement preventive measures with planned resilience – the ability to respond and recover when attacks do happen. Resilience includes the advance determination of procedures to manage incidents, as well as rehearsals and exercises to make sure those procedures work. It is also important to integrate cybersecurity resilience with existing crisis response plans, so senior leaders will be brought into the process when necessary and other players such as suppliers and operational staff will get the information and instructions they need.

Invisible assets, inestimable harm

With few exceptions, the world political and business leaders who will ultimately be responsible for ensuring global cybersecurity are members of the analog generation. They came to maturity at a time when most stores of value were visible and tangible. Most leaders have an intellectual understanding of the stakes in global cybersecurity, but they may be less inclined to "feel" the magnitude of the threat, or the urgency of the situation. Some comparative arithmetic may put the situation in perspective.

Consider other risks that have been met with a coordinated international security response. The recent rash of maritime piracy incidents off the coast of Somalia, past which about 10 percent of the world' sea trade passes,[5] is said to have netted pirates approximately US$150 million in ransom payments from November 2007 to November 2008,[6] and the international community has responded by sending warships from more than 20 nations to the area at a cost estimated at between £150 and 250 million annually.[7] Globally, the passenger aviation industry is projected to take in US$467 billion in 2009,[8] and the daily operation of that system is protected by extensive and well-established multinational protocols for safety and security.

How large is the global cyber economy? It may be impossible to say. But the electronic storage and transfer of data has become entwined with almost every part of personal and public business in most nations. And the Gross World Product in 2008 has been estimated to total more than US$70 trillion.[9]

With few exceptions, the world political and business leaders who will ultimately be responsible for ensuring global cybersecurity are members of the "analog generation."

What degree of international investment and cooperation is appropriate to safeguard that economy? One might as well ask, what degree isn't? Managing global cyber risk will be far

more complicated than thwarting Somali pirates or standardizing aviation safety. But that complex work won't succeed until leaders around the world fully embrace the size and urgency of the issue.

More than data is at stake

In addition to its many specific policy goals, the new U.S. administration has promised the world a new regime of openness and transparency. This goal was born in part from the advanced, Web 2.0 campaign that brought the administration to power by reaching a new generation of digitally enabled voters. But the benefits of a more open approach aren't limited to the United States, and they go far beyond the symbolic.

When information flows freely among different organs of the government, they perform more efficiently. When it can flow between the government and private sector with minimal restriction, people can get more out of the systems their tax dollars support. When governments and companies can feel secure using international channels of communication, commerce and cooperation can flourish.

The traditional approach to cybersecurity – building walls – fails these tests. Yet a culture of openness fails to address threats as they're traditionally defined. To move forward, the public and private sectors must work together to develop a new operating model that avoids both extremes.

Cybersecurity or cyberprotectionism

Traditionally defined "protectionism" is the deliberate erection of barriers that prevent commerce. If effective international cybersecurity isn't put in place, the result could be a new growth of "cyberprotectionism" that combines both intended and unintended curbs on trade.

If disparities in cyber risk management persist from one country to another, some governments might deny potentially unsafe trading partners access to their domestic economies. Conversely, companies or governments might shy away from operating in overseas markets where they don't feel their assets will be protected. Even when actors on the international economic stage find the risks to be manageable, the necessary safeguards add cost. In trade, cost represents friction and slows the system.

The solution lies in uniformity, and achieving it will require trust and collaboration. There is less risk in allowing information and digital value to cross borders if it is handled with the same stringent security everywhere – if there are no inconsistencies for wrongdoers to take advantage of.

The case of port security can be instructive. When global customs standards imposed requirements that some vital trading countries could not afford to meet, the world's leading industrial nations subsidized their compliance so that security would be comparable at all points in the chain. With cybersecurity, the solution may or may not involve a similar degree of material cooperation, but it must include the same uniformity of standards.

Physical shipping, for all the risk management it entails, has a high cost of entry because of the capitalization required. The cyber economy has virtually no barriers to entry, apart from the purchase of a computer and Internet access. So miscreants start out with an advantage – all the hard costs are borne by the other side. And a risk accepted in only one nation affects the entire system.

The roles of the public and private sectors in securing cyber resources are inextricable

In an administrative sense, if not a metaphysical one, government is the source of identity. Much like paved roads, clean water or stable currency, secure identity is a precursor resource that makes it possible for people outside of government to get things done. Yet most of the online infrastructure that uses and verifies personal identity is in private-sector hands, and it doesn't seem likely that the public would accept a government takeover of these processes.

How can government carry out its responsibility to protect the value of an information resource that it originates but does not control? By setting standards that build better security into identity, so that its users can operate more confidently in private transactions. While many of the possible outcomes are technical, such as biometric access control for Internet use, they must arise from a higher-level conversation that addresses societal considerations before focusing on the ones and zeroes.

For example, a new approach to secure identity might include not only ways to thwart identity theft, but to detect and report it – so that individual citizens could receive identity threat alerts in much the same way that they receive credit report alerts today. And laws governing data privacy must align with the new reality – recognizing both the threats and the possible remedies – so that technical and legal safeguards work hand in hand to protect people and institutions.

Access to an economy from the outside, like identity, is one of the precursor resources that government administers for the sake of non-government actors. Governments around the world already carry out this function in a number of well-established ways: They don't allow the importation of tainted meat, dangerously infected people, or untested pharmaceuticals.

It's time to add cybersecurity to that list. Access to a nation's economy can and should be made contingent upon adherence to that nation's cybersecurity standards and protocols. While this may be a new requirement, it would be consistent with the traditional role governments play in safeguarding the playing fields under their jurisdiction.

A view from the front lines

Lt. General Harry D. Raduege (USAF Ret.) was Director of the Defense Information Systems Agency and Manager of the National Communications System. He served 35 years in the U.S. military, and worked in the areas of technology, including telecommunications, space, information and network operations. He also led the nation's efforts to prioritize the restoration of telecommunications throughout New York City and the Pentagon following the 9/11 attacks. Today he is the Chairman of the Deloitte Center for Network Innovation.

Cybersecurity is a critical issue in the world today – and, for good reason. Cybercrime now exceeds drug trafficking in criminal activity and estimates are that the damage from global loss of data through the cyberspace domain exceeds $1 trillion a year.

While we all operate daily in cyberspace, we are confronted with two opposing dynamics.

On one hand, in order to perform more effectively and efficiently, we are encouraged to collaborate and share information more freely, to derive the benefits of cloud computing, and to employ Web 2.0 tools. In effect, we are evolving into an Age of Interdependence.

On the other hand, this state of openness in business operations is presenting a new set of targets for cyber pests, warriors, criminals, and spies. Only by creating a new "cyber mindset" will we be able to counter the exponential financial and national security losses being incurred from growing rates of cyber disruption, crime, & espionage. Cybersecurity has become a new prerogative for successful business operations, whatever your organization does.

A reality of cyberspace today is that outsiders can gain access to your information networks and databases. In order to secure your future in cyberspace, everyone needs to learn how to manage the risk associated with cybersecurity. Through proper risk management and public private partnership we will be able to secure a future in cyberspace.

Incentive and accountability - government influence over private actors

Governments can also use incentives to bolster the private sector's approach to cybersecurity. Certainly there is a need for regulation – for "rules of the road" analogous to the ones that govern other forms of commerce. But there must be a proper balance between inducing the right behavior and inviting the negative effects of over-regulation, and there are other, more positive ways government can influence private actors. If government can contribute to the creation of reliable metrics for cybersecurity, private operators such as Internet Service Providers (ISPs), equipment manufacturers and software designers would be able to use those metrics to establish competitive advantage. Tax breaks, preferred access to government contracts, and performance-based rewards are other potential measures that can encourage business to do its part in balancing the freedom of the Internet with the safety of its users.

Expecting private-sector participants to take part in maintaining security isn't unprecedented. Nor is the idea of giving them competitive advantage for taking on that responsibility. In most developed countries, a recognized governing body – such as TÜV organizations in Europe or Underwriters Laboratories (UL) in the United States, which have been in operation for more than a century – certifies the safety of consumer products, whose manufacturers then may display a seal on their products and advertisements. Such a system, which gives individual and institutional consumers confidence in the products and services they purchase, could conceivably be applied to digital equipment that meets standards for cybersecurity.

The balance between security and civil liberty should be gauged by performance, not by rhetoric

Has the safeguarding of the world's commercial air transport been a success or a failure? The early results of post-9/11 measures included difficulties such as long lines, delays, and vocal public dissatisfaction. But governments persisted in establishing a rationale for the new system – making it a de facto "brand" that influenced public awareness – and in 2006, the U.S. Transportation Security Administration screened more than 700 million travelers and more than 500 million pieces of checked luggage. Evidently people recognized the need, voted with their feet and went to the airport in spite of the new inconveniences. And in more than

seven years, the attacks that brought the TSA into being have not been repeated.

Moving a society toward a new understanding of cybersecurity is likely to involve analogous changes to long-established habits. Ordinary citizens, in their home and work lives, may be called upon to use computers and the Internet in ways that are less convenient and permissive than they do today. And people will complain. But they will keep using them – and if the new policies are well thought out, they will eventually find greater utility in a system that is safer to use than it used to be.

Know and address the sources of cyber threats

Espionage and theft are common archetypes of cyber threat, but in practice, threats come from different vectors – and arise from many causes. Meeting the threat at its source is an effective complement to defeating it on your own turf.

If you identify the type of person who may seek to harm your systems, you can use policy to defuse the problem at its source.

In the case of deliberate attack, someone has a motivation to act. A comprehensive cybersecurity policy should anticipate these motives and seek ways to deflect them. Not so easy perhaps when your prospective opponent is an antagonistic nation-state, but more difficult if you are facing an ideological movement or non-state actor. Or a disgruntled employee or contractor. The current economic crisis adds fuel to a number of possible motivations for cyber-wrongdoing, including industrial espionage, dissatisfaction with employers, or simple lucre.

If you identify the type of person who may seek to harm your systems, you can use policy – not technology measures, but the full spectrum of means available to government – to defuse the problem at its source. Create a situation in which the would-be cyber-attacker gets a better return on his or her time by doing something else. We speak of a strategic, comprehensive, holistic approach to cybersecurity, and this is about as broad as it gets.

Not all threats are external, and not all are deliberate. When the risk to information systems comes from within, one of three causes is involved: complacency, arrogance, or intentional harm. For the first two, education and involvement are effective countermeasures. In wartime generations ago, posters warned port city residents were warned not to speak openly of shipping departures, for fear that enemy spies would relay the information to waiting submarines. Today, the threats and the means to combat them are more complex – but the principle of individual responsibility is the same.

Governments shouldn't make the mistake of explicitly looking only to explicitly international programs or processes when applying new standards for cross-border cybersecurity. Certainly a trade relationship or military alliance raises these concerns, but other operations that appear domestic may actually involve significant foreign contact because of global supply chain systems or services offshoring. It may be best to do away with the idea that anything ever happens without some exposure to other nations.

Remember also that no matter how much we speak of new paradigms, holistic approaches and society-wide awareness, the old threats to cyber assets remain in place. People will steal files, use default passwords from the factory, leave notebook computers in their cars, and write their passwords on their cubicle dividers. Don't allow a new, broader outlook on cybersecurity to trump effective measures you've relied upon for years.

What will experts on cybersecurity tell us five years from now that we could have, should have, done today?

If everything is critical, nothing is

This may sound like a call to selectively ignore some elements of the cybersecurity threat. In fact, it's a call to treat it comprehensively – as a design problem. It's unlikely that cybersecurity resources will ever outnumber cyber threats. What do you do if you have $10 to spend and $100 worth of places to spend it? Prioritize.

Define the problem more intelligently. If you can identify the elements of your infrastructure that are most critical, and most susceptible to deliberate or accidental cyber failures, you will be able to allocate security resources for the best overall protection of the systems under your jurisdiction. Most people know that in America, the TSA eventually ended its prohibition of small, sharp items like fingernail clippers on commercial aircraft. It's less well-known that while the rule was in effect, the agency found it was spending a disproportionate number of man-hours confiscating items that didn't pose a risk of bringing down an aircraft.

If the goal is to keep an airplane from becoming a missile, start with the cockpit door and let people have their nail clippers. If our goal is to prevent error, complacency and malfeasance from compromising Internet security, similar choices lay before us. To be effective, cybersecurity must be an art of the possible.

It can also be an art of the clever. During the development of the first atom bomb during the Second World War, workers knew only their own small parts of the job – only the top leaders knew what was really happening Today, some large media producers use similar compartmentalization to keep their creative output from being fully assembled until the very end of the process. So it's harder for any one person to steal something useful. Instead of shipping dangerous chemicals through populated areas, carriers take every opportunity to keep non-lethal components separate until they arrive at the point of use. What structural lessons can cybersecurity practitioners learn from these and other examples?

Lessons from the financial meltdown

As the global financial crisis dominates the headlines, much of the dialog is backward-looking. Many hands are wrung on television every day over what regulators and private-sector players could have done months or years ago to avert the current trouble. If only they'd known.

The parallels between cybersecurity and the financial sector are worth considering. Both involve critical decisions about the relationship between the public and private sectors, the correct use of top-down regulation, and the balance between individual liberty and the common good. Both topics lay bare the illusion that modern problems stop at ancient borders, and teach us that transnational problems require transnational solutions. And both illustrate the value of communication, cooperation, and identifying threats while they're still on the horizon.

Perhaps the most urgent lesson the financial crisis can teach leaders about cybersecurity is the need for decisive action. Waiting for a complex system to self-correct – for "everything to work out" – is a recipe for trouble.

What will experts on cybersecurity tell us five years from now that we could have, should have, done today?

Conclusion

Several nations, including the United States, Canada and the United Kingdom, are at various stages of reviewing and implementing new approaches to cybersecurity. The order for the U.S. review included a mandate to integrate new cybersecurity initiatives with the private sector. In Deloitte member firms' view, this type of integration and coordination will be vital to success in every country. No nation's policy on cybersecurity can succeed if it is limited to technology, to government, or to strictly defined protocols.

One national cybersecurity leader recently compared the cybersecurity problem to a Gordian Knot. That legendary metaphor is useful as a description of how complex the situation is, but it is not prescriptive – because in the story, no one could untie the knot, and Alexander solved the problem with a stroke of his sword.

In our reality, the cybersecurity "knot" won't be "solved" with a single master stroke, and it isn't going away. Rather, our challenge is to live with the knot – to navigate its complexity and find the opportunities within. The risk is part of almost every public and private interaction. The solution must be cast just as broadly.

Deloitte member firm cybersecurity leading professionals that were interviewed for this document

United States

- **Rich Baich**, Principal, Security & Privacy Services, Deloitte United States (Deloitte LLP), and former Naval Information Warfare Officer for the National Security Agency (NSA)
- **Marshall Billingslea**, Strategy & Operations Director, Deloitte United States (Deloitte LLP) and former Deputy Under Secretary of the Navy
- **William "Billy" O'Brien**, Manager, Deloitte United States (Deloitte Consulting LLP), and former Director, Cyber Security and Communications Policy at the White House
- **David L. Brant**, Director U.S. Federal Practice, Deloitte United States (Deloitte LLP), and former Director, NCIS
- **Michael G. Gelles**, Human Capital, Deloitte United States (Deloitte Consulting LLP), and former Chief Psychologist for the Naval Criminal Investigative Service
- **Gary McAlum**, Senior Manager, Security & Privacy Services, Deloitte & Touche, LLP (Deloitte US) and Colonel (retired), United States Air Force-
- **Greg Pellegrino**, Global Public Sector Industry Leader, Deloitte Touche Tohmatsu
- **Harry D. Raduege (USAF Ret.)**, Chairman of the Deloitte Center for Network Innovation, Deloitte United States, Deloitte LLP, and former Director of the Defense Information Systems Agency

Europe

- **Steve Cummings**, Special Adviser, Enterprise Risk Services, Deloitte UK, and former Director of the Centre for the Protection of the National Infrastructure
- **Chris Verdonck**, Partner , ERS EMEA Practice Leader, Deloitte Belgium
- **Ward Duchamps**, Deloitte Enterprise Risk Services, Deloitte Belgium

Asia/Pacific

- **Piti Pramotedham**, Partner, Risk Consulting, Deloitte Singapore
- **Oliver Binz, Partner**, Security and Privacy Services, Deloitte Australia

Latin America

- **Andrés Gil, Partner**, Security Services, LATCO, Deloitte Argentina
- **Mauricio Romero**, Consulting Partner, Security & Privacy services, Deloitte Mexico

Canada

- **John Detombe,** Associate Partner, Deloitte and Touche LLP, Deloitte Canada

What is at stake?

International Relations and National Infrastructure

Cyber attacks are now being used by governments as another way to counter opposition. In 2007, hackers crashed the Estonian government's networks, and Web sites of the government, political parties, media and business community had to shut down temporarily. The attacks reportedly originated in Russia, after Estonia moved a controversial Soviet-era war memorial. Russia also was blamed for an August 2008 attack against Georgia, which marked the first time cyber attacks coincided with actual military attacks. China is also suspected to be responsible for Distributed Denial of Service attacks against the U.S. Department of Defense in 2001, which were believed to have been launched against the U.S. Pentagon's network after the 2001 collision between a U.S. Navy spy plane and a Chinese fighter jet, forcing the Navy plane to land in China. CNN's Web site suffered similar attacks after one of the network's reports made disparaging comments about China hosting the Olympic Games.

Specific individuals

Deliberate compromises to Internet security can be targeted down to the individual level – including highly placed individuals such as U.S. senators Bill Nelson (D-Fla.) and Frank R. Wolf (R-Va.), both of whom have reported security breaches of their office computer systems. Senator Nelson's office traced the attackers' internet protocol (IP) addresses to China, though they could have been masked. U.S. presidential candidates John McCain and Barack Obama both suffered attacks against their individual campaigns' networks in 2008 as well.

Corporations and Economy

Disgruntled employees with access to an organization's cyber systems can do significant damage. In January 2009, a fired employee of the Federal National Mortgage Association (Fannie Mae) was charged with attempting to shut down the firm's servers by attaching malicious code to a daily programming routine. The code was discovered by accident, and would have stopped business for at least a week. The slowing economy and rising unemployment rate will most likely increase the motivation for similar attacks, driven by either hope of financial gain or simple vengeance. Organizations may also have to deal with the economic impact of reputation and branding image.

Governments

One might expect the U.S. President 's residence –the White House– to be one of the most cyber-secure places in the world. Yet hackers from abroad have penetrated the White House computer network on multiple occasions, maintaining access long enough to obtain e-mails between government officials and other information. As with similar attacks elsewhere, U.S. government experts suspect the attacks originated in China, but cannot trace them with certainty.

Appendix
Regional views on cybersecurity

Threats to cybersecurity and the culture it enables are a global phenomenon, and each region and country has its own perspective on the problem. According to a panel of cybersecurity leading professionals from Deloitte member firms from around the world, governments everywhere should consider action immediately. This is what Deloitte Touche Tohmatsu heard from them about cybersecurity concerns in the areas they serve.

Data crosses borders instantly. Cultural, legal and technical safeguards often begin or end at the frontier. In some parts of the world – even in regions that are economically robust and technologically advanced – cultural awareness of the threat may not be what others expect. Laws to protect the privacy of data may not be in place, or may differ significantly from region to region.

Asia-Pacific

Cybersecurity in this part of the world is marked by a great variety in approaches from nation to nation, and there are benefits to be realized if standards for security were made more similar across the region. In general, the region is marked by a comparative lack of protective legislation and cultural awareness when compared to its rapidly growing technology and connectivity.

Singapore, for example, has a significant cyber culture marked by compulsory use of a national identity card. In 2008 the government there launched a US$70 million Infocomm Security Masterplan that encompasses hard cyber assets, widespread competence and awareness, public-private cooperation, and international collaboration. Australia has no such national identification system – a smart driver's license pilot program is underway in the state of Queensland – but its government and corporate cybersecurity approaches are analogous to measures in widespread use in the United States and Europe. Thailand, Malaysia and other nations have devoted fewer resources to cybersecurity, and there are opportunities to make safeguards more uniform through increased international cooperation.

Legal cooperation is another area for improvement, as strained relationships and disparities in criminal law make it difficult to pursue cyber criminals across borders, or even to identify the real culprits. In particular, the minimal observance of data security and international IP law in China is a source of concern that calls for greater security in other states. In general, the region needs to strengthen safeguards against the economic drain associated with intellectual property loss. A 2008 study found that when Japan's data is removed from the equation, the Asia-Pacific region's financial sector suffers from a higher rate of security breaches than the world average, but invests less in security and privacy training for employees.

Thailand, Malaysia and Singapore are examples of states in this region that attract medical tourists from the West. People who arrive to combine a vacation with affordable medical treatment may enjoy the convenience, but they may also arrive expecting a Western standard of data privacy legislation that is actually not in place. Protecting private medical records should be a priority for governments in the region.

In general, Asia-Pacific cybersecurity needs to catch up to the other economic engines, such as human talent and technology infrastructure, that are powering the region's vitality. If the proper investments aren't made, cybersecurity could become the weak link that stalls growth.

Europe

Denial-of-service attacks in Estonia in 2007 and Georgia in 2008, coinciding with well-publicized (and in the Georgian case, violent) international conflicts, have made Europe the site of the first widely recognized "cyber wars." It is not a coincidence that these attacks happened on the continent: Both Georgia and Estonia had made significant investments in IT-based citizen services, so they were vulnerable to disruptions that had significant, immediate effects on the working public. And each was in conflict – one diplomatic, one violent – with an adversary that had the capability for cyber attack within its borders.

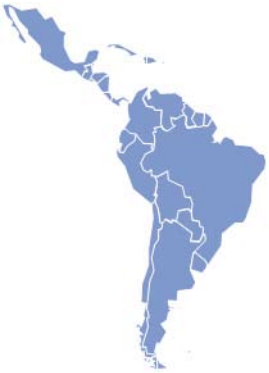
The United Kingdom is in the process of writing a national cyber strategy with emphasis on public-private partnership. On the continent, the European Commission has called upon member states to coordinate cybersecurity measures including information sharing, contingency plans, and disaster and recovery exercises. The European Network and Information Security Agency (ENISA) has pledged to support the effort.

NATO has also taken a significant role in addressing cybersecurity policy, though its influence is felt more keenly in new member states. In fact, NATO established its Center for Cyber Defense in Estonia, target of the 2007 attacks. One element of the alliance's approach has been to encourage greater cooperation among nations in responding to cyber attacks.

Europe's advanced electronic connectivity and many borders mean that companies and governments there frequently rely on systems and networks that are located in other states, often with different legal and cultural approaches to security. There is significant opportunity for efforts that would standardize the approach to cybersecurity, in turn enabling a freer approach to business transactions.

In general, cybersecurity in Europe is characterized by disparity – from one nation to the next, there are often significant differences in experience and capability. Because cross-border activity is so central to life in the region, and because of the need to defend against cyber-attacks has already been demonstrated, cooperation and alignment should be a priority.

Further, the region's recent experience with explicit cyber war may have desensitized some policymakers to the more insidious effects of smaller, everyday threats.



Latin America

Diversity of approaches and resource levels is a characteristic of cybersecurity in Latin and South America as well.

In Mexico, cybersecurity is presently viewed as primarily a concern for the financial sector, and government is working to foster a culture that prizes broader cybersecurity as an investment, not a cost. Government bodies there work closely with private contractors to handle cybersecurity as a managed service, and government agencies are now required to include a formal security structure in their leadership. Attempts to compromise financial data systems in Mexico frequently have a political element, as the private information taken from accounts is sometimes prized more than the money. Argentina is also considering legislation

that would mandate security organs within government entities.

Politics is a factor elsewhere in the region's cybersecurity picture – and an opportunity. In nations whose people may be mistrustful of government because of real or imagined corruption, the transparency enabled by secure data channels can lead to greater confidence and more effective and efficient use of online government systems.

Canada

The Canadian approach to cyber security is focused on three primary initiatives: protection of government and continued improvement to government systems; support to Critical Infrastructure sectors and broader private sector community; and fighting cyber facilitated crime and supporting end users and private citizens. Public Safety (PS) Canada, a federal government department, is responsible for policy development and advising the government on matters of national security, and has within its mandate the development and implementation of a National Cyber Security Strategy. The development of this strategy was initiated with a two-year Cyber Security task force. A key component of the cyber security strategy is the creation of a new Directorate of Cyber Security with a mandate, in part, to engage closely with the private sector. This directorate is scheduled to begin operations in 2009. The Canadian strategy, like other nations, is focused, in part, on critical infrastructure protection and the organizations that make up that infrastructure. Another area of focus is to establish close relationships with the CEOs of the country's firms in order to foster the trust that will encourage information sharing between the public and private sectors pertaining to cyber security and cyber threats. This information sharing is seen as a critical aspect of a successful cyber security strategy.

United States

A 60-day comprehensive review of national cybersecurity policy ordered by President Obama has recently concluded, and this effort follows other investigations such as a Comprehensive National Cybersecurity Initiative (CNSI) in early 2008, a report from the Center for Strategic and International Studies, and Congressional hearings.

As in Europe, there is a need for U.S. planners to embrace not only the "one big attack" mentality encouraged by recent events, but also a more comprehensive, day-to-day cybersecurity strategy. As an open society with a significant knowledge-based economy and a military spread physically across a large part of the globe, the United States must make intellectual property loss a priority.

End notes

Main body

[1] "Major cyber spy network uncovered." BBC News Americas. 29 Mar. 2009. BBC. 12 Apr. 2009 <http://news.bbc.co.uk>.

[2] "China capable of launching cyber attack on UK." The Economic Times. 29 Mar. 2009. 12 Apr. 2009 <http://economictimes.indiatimes.com/>.

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

[4] Cooper, Charles. "Data about Obama's helicopter breached via P2P?" CNET News. 28 Feb. 2009. 12 Apr. 2009 <http://news.cnet.com>.

[5] Axe, David. "Beating Somali Pirates at their Own Game." Wired. 6 Apr. 2009. 12 Apr. 2009 <www.wired.com>.

[6] "Pirates 'gained $150m this year'" BBC News. 21 Nov. 2008. 12 Apr. 2009 <http://news.bbc.co.uk>.

[7] 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>.

[8] Pringle, Chanel. "Global airline industry to suffer $4,7bn loss this year – Iata." Creamer Media's Engineering News. 24 Mar. 2009. 12 Apr. 2009 <http://www.engineeringnews.co.za>.

[9] "World." CIA - The World Factbook. 9 Apr. 2009. 12 Apr. 2009 <https://www.cia.gov>.

"What is at stake?" section

International Relations and National Infrastructure – O'Connor, Fred. "Political cyberattacks to militarize the Web." ComputerWorld. 12 Mar. 2009. IDG News Service. 13 Apr. 2009 <http://www.computerworld.com>.

Specific individuals – Rogin, Josh. "Hackers Based in China Break Into Florida Senator's Office Computers." CQ Politics. 20 Mar. 2009. Congressional Quarterly. 13 Apr. 2009 <http://www.cqpolitics.com>.

Corporations and Economy - Gorman, Siobhan. "Virus was set to destroy Fannie Mae data." Wall Street Journal [New York] 31 Jan. 2009: A2.

Governments – Sevastopulo, Demetri. "Chinese hack into White House network." Financial Times [London] 7 Nov. 2008.