Written Testimony of
Scott Charney
Corporate Vice President, Trustworthy Computing, Microsoft Corporation

Before the
Senate Committee on Homeland Security and Governmental Affairs
Hearing on "Securing America's Future: The Cyber-Security Act of 2012"

February 16, 2012

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for the opportunity to appear today at this important hearing on cyber-security. My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft. I currently serve on the President's National Security Telecommunications Advisory Committee (NSTAC), and I previously served as one of the co-chairs for the Center for Strategic and International Studies (CSIS) Commission on Cyber-security for the 44th Presidency.

Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. During my government service, I oversaw every major hacker prosecution in the United States from 1991 to 1999, worked on major legislative initiatives, and Chaired the G8 Subgroup on High-Tech Crime and other international efforts.

Cyber-security is an important issue for America, other nations, the private sector, and individuals. I have had the privilege of testifying before Congress about cyber-security several times[1]. In an effort to better understand the challenges we face, I regularly engage with government leaders from around the world, security-focused colleagues in the IT and Communications Sectors, and companies that manage critical infrastructures. Based on these interactions, it is my opinion that cyber-attacks have joined terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts the U.S., its allies, its corporations, and its citizens at risk. I commend this Committee and the members of the Senate for your continuing commitment to addressing one of America's most complex national and economic security challenges. You and your staff have created a venue for private sector input into deliberations on cyber-security, which is essential given that the private sector owns and operates most of this country's critical infrastructure.

[1] Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing "Securing America's Cyber Future: Simplify, Organize and Act" Before the House Committee on Homeland Security Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology Hearing on "Reviewing the Federal Cybersecurity Mission" (March 10, 2009).

Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing "Securing America's Cyber Future: Simplify, Organize and Act" Before the House Committee on Homeland Security Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology Hearing on "Reviewing the Federal Cybersecurity Mission" (March 10, 2009).

It is my view that the current legislative proposals provide an appropriate framework to improve the security of government and critical infrastructure systems and establish an appropriate security baseline to address current threats. Furthermore, the framework is flexible enough to permit future improvements to security − an important point since computer threats evolve over time.

My testimony will begin with a brief discussion about the transformative effect of the Internet, as well as the challenges facing policymakers. Then I will discuss the three key outcomes that U.S. national policy and legislation should promote to improve resiliency in the near-term, and ensure continued innovation and leadership in the long-term. These three outcomes are:

1) Flexible and agile risk management, narrowly focused on risks of greatest concern and optimized to adapt to rapidly changing threats;

2) Innovative information sharing, targeted to address specific challenges and enable advanced risk management, response, and recovery capabilities; and

3) Meaningful and attainable international norms for the security of cyberspace.

The Transformative Challenge of Cyber-Security

The Internet continues to transform America and the world, with both positive and negative effects. Its decentralized architecture, open standards, and extensibility have created a global platform for communication, commerce, and innovation. Indeed, the United States is perhaps the best example of how the Internet can enhance productivity and commerce, as well as enable new forms of social and political engagement.

At the same time, today’s Internet has a thriving underground economy with its own specialized roles and needs. For example, researchers may helpfully identify new product and system vulnerabilities, only to have cyber criminals use that research to develop and launch malicious code causing significant harm. We have also seen a rise in social engineering; attackers trick trusted employees into opening infected email attachments thereby planting malware on targeted systems. We have also seen attacks against the “trust mechanisms” designed to ensure security across the Internet ecosystem, such as the attacks against companies that provide security certificates for machine-based authentication and safer web browsing. Whether these bad actors are engaged in crime, economic espionage, or military espionage, or are otherwise supporting military objectives, the salient point is that governments, enterprises, and Internet citizens face an environment where cyber risks are often hard to understand and manage.

To respond effectively, the United States must integrate and harmonize its cyber policies, recognizing that actions taken by the United States Government will have ramifications beyond its own borders. The United States must ensure that its cyber policies are technology neutral and do not stifle innovation; and it must promote meaningful and cost-effective risk management techniques and adapt them to the unique nature of cyber risks. Success in the long-term will also ultimately depend on building a workforce – and future leaders – for the Information Age.

The need to integrate and harmonize cyber-security policies is, in part, a byproduct of the Government's progress in cyber-security. In prior testimony to Congress on cyber-security, I highlighted the need for a national cyber-security strategy that aligned all elements of national power: economic, diplomatic, law enforcement, military, and intelligence. I further stated that the strategy must articulate how those elements would be employed to ensure national security, economic security, and public safety, and to assure delivery of critical services to the American public. At that time, the body of U.S. cyber-security policy was relatively thin.

Over the past few years, the Government has moved incrementally to improve its cyber-security posture. First, the Comprehensive National Cybersecurity Initiative set the baseline for American operational and strategic readiness, and we have since seen an array of policy documents that chart a course ahead. The White House's International Strategy for Cyberspace and National Strategy for Trusted Identities in Cyberspace, the Department of Defense's Strategy for Operating in Cyberspace, and the Commerce Department's efforts on privacy, cyber-security, intellectual property, and the global free flow of information demonstrate the Government's commitment to driving cyber-security policy forward in the right direction.

However, we have not always seen alignment or harmonization between these different strategies. While each initiative has value, their long-term effectiveness would be improved by an articulation of common goals and operational alignment to maximize their impact. It is clear that cyberspace demands a different type of policymaking; agencies cannot develop and implement policies in silos. Nor can national governments act alone. The Internet is truly global and the U.S. Government must be cognizant that American cyber-security efforts reverberate beyond our borders. In some instances, foreign governments will act in alignment with American interests and may even emulate its policies. In other instances, however, there may be disparate national approaches. Countries may have philosophical differences, of course, but sometimes technical requirements – even if promoted in the name of national security – are really attempts to create trade barriers. Policymakers must be mindful of the global import of their actions and ensure that competing interests are balanced appropriately.

More specifically, America must set an example and define cyber-security policies that are technology-neutral and do not stifle innovation. Technology-neutral policies do not promote, require, or otherwise advance a particular technology product or set of products to the exclusion of others; rather they identify desired outcomes and allow the marketplace to find the most innovative way to achieve those outcomes.

To meet these challenges ahead, the Government must catalyze the growth of leaders who can drive excellence in cyber-security. By providing new incentives for STEM education, particularly security-focused education, the Government can ensure that America has the talent necessary to be a leader in technology, innovation, and policy. Title IV in the current legislative proposal recognizes this need and initiates actions across the Federal government, academia, and industry to drive improvements. The future workforce must be able to address cyber risk management in the public and private sectors, as well as serve the needs of law enforcement and intelligence. Moreover, we need a diplomatic corps and policymakers that grasp technology, as well as its impacts in the evolving geopolitical landscape in cyberspace.

Flexible and Agile Risk Management

Globally, governments, enterprises, and individuals depend on the information infrastructure and the data that IT systems contain, and there are often no alternative physical means to perform core functions. Yet, as discussed above, the information infrastructure faces a myriad of ever-changing cyber threats.

There is broad agreement, well reflected in various legislative proposals, that risk management is the appropriate approach to improve the security of the critical infrastructures on which we all depend. There are simply not enough resources or time to address all the risks we face. Yet while risk management is a well understood discipline, managing cyber risks is particularly difficult. This is because cyber risks are complex, it is difficult to quantify those risks and the value of potential mitigations, and it is important that we not hinder innovation and agility.

I have previously written about the challenges of understanding cyber threats and managing cyber risks,[2] so I will only summarize the key points here. While there are many malicious actors and motives, the attacks often look alike (that is, you cannot discern the actor or motive from the nature of the attack). The speed of attack may surpass our ability to respond, and responses are complicated by the fact that the Internet is a shared and integrated domain (it is shared by governments, businesses, and individuals, and the Internet is used to engage in a wide range of conduct from constitutionally protected activities to illegal acts). Finally, the potential consequences of an attack are very difficult to predict; and the worst-case scenarios are alarming.

By way of example, the market for cyber-security insurance is remarkably small, particularly given the tremendous reliance upon IT products in our daily lives. For many enterprises and even consumers, IT investments and products are at least as valuable as other assets for which insurance can be purchased. Yet, insurers are reluctant to provide coverage for cyber-incidents for a simple reason: cyber-security risk is nearly impossible to measure.   The complexity, massive interconnectivity, and dependencies between systems, companies, and sectors are not well understood, and we lack sufficient data and expertise to determine with confidence the likelihood and probable consequences of a successful attack.

Therefore, while we must continue to anchor our approach to securing the information infrastructure in risk management, we must also evolve how that discipline is applied to better address the unique nature of cyber risks. When doing so, government and industry need to ensure that their approach is appropriately scoped to address pressing national security and public safety concerns, and also remains sufficiently flexible and agile to enable organizations to manage risk in a dynamic cyber threat environment.

[2] Scott Charney, "Rethinking the Cyber Threat – A Framework and Path Forward." http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=747 (May 3, 2010).

When considering how to effectively manage cyber risks for the information infrastructure, government must balance dual, and often interrelated, roles. First, as a public policy entity, the government is responsible for protecting public safety, as well as economic and national security and must consider which infrastructures support those missions. But the Federal government is also a large and widely distributed enterprise, with countless globally distributed customers (e.g., citizens who want to connect with their government), partners, operations, networks, and resources. Although distinct, the policy and enterprise roles are not entirely separate, as each affects and informs the other.

Government and industry must be particularly careful when delineating the elements of the information infrastructure that are truly critical to national security and public safety. While we cannot eliminate all risks, we must ensure the highest priority risks are addressed. Each risk should be assessed to determine its severity, the consequences of a successful exploit should be understood, and the likelihood of harm should be evaluated. Appropriately identifying the infrastructures that should be covered and the risks to be addressed will enable both government and private sector leaders to better secure the nation's critical information infrastructure.

Similarly, we must create a risk management framework that enables the agile responses necessary to respond to rapidly changing cyber threats. It is important to understand that risk has historically been managed by focusing on "verticals" (e.g., banking, health care) but information technology runs horizontally underneath all verticals. We therefore need a risk management model that (1) recognizes this horizontal layer (that is, IT risks need to be managed in common ways), but (2) appreciates that verticals have unique requirements. We therefore recommend a hybrid model that includes:

- A centrally managed horizontal security function to provide a foundation of broad policy, security outcomes, and standards; and

- Vertical security functions resident in individual organizations to enable them to manage their unique risks with agility.

This combination of horizontal and vertical functions ensures that minimum security goals and standards are set, yet provides organizations with flexibility to manage the unique risks associated with their operating environments.

This hybrid model is relevant to how the U.S. Government should manage cyber risk for the Federal enterprise as well as those narrow sets of systems designated as critical infrastructure. Moreover, while this hybrid model works well for both government and critical infrastructure, its implementation, and in particular the oversight and audit responsibilities, should differ. This is because the private sector has a more diverse set of business functions and, I think it is fair to say, moves at a faster pace.

The Federal government requires the hybrid model for risk management precisely because it is a large collection of businesses with different missions, partners, customers, data, assets, and risk; in other words it can and should be managed as an enterprise. While there are some responsibilities and practices that should be commonly undertaken by each and every

Federal agency, different agencies may also have unique security requirements and concerns. Thus, there should be centralized oversight to ensure horizontal requirements are established and met, as well as agency flexibility so that unique needs can be addressed.

The complexity of the IT systems and data that span and support America's critical infrastructure far exceeds that of the Federal government. Enterprises, large and small, also deliver critical functions and innovations at an unprecedented speed, and in an increasingly competitive global environment. These infrastructures are remarkable for more than their speed; their collective operations ensure public health and safety, and underpin the entire economy. Due to this fact, it is clear that critical infrastructures also have areas of commonality and areas of difference. Thus, in order to continue enabling these infrastructures to drive the economy forward, regulators should take the outcomes defined for the horizontal plane and also consider the unique implementation requirements in each sector. This approach – which does not establish a new regulatory authority – is important, as dealing with two sets of regulators would divert resources that should be devoted to security.

Having reviewed both the title seeking to reform the Federal Information Security Management Act, as well as the title focused on protecting critical infrastructure, we are encouraged to see that the proposals leverage this hybrid model, which we believe will advance security.

While appropriately tailoring the role of government, we must remain cognizant that cyber-security needs to be improved beyond just critical infrastructure. To do so, government and industry need to set the strategic context and define reasonable cyber-security goals and objectives. These objectives could form the basis of voluntary codes of conduct—a collection of recommended security goals and objectives that, if appropriately incentivized, would drive adoption of standards and widely accepted industry practices and, therefore, raise the level of cyber-security both nationally and internationally.

Innovating Information Sharing

Successful risk management depends on effective information sharing. However, over the past 10 years, several attempts to improve operational coordination between and among key government and private sector stakeholders have met with limited success. Additionally, legislative and policy efforts designed to encourage the private sector to share cyber-security information with government agencies have met with equally limited success.

That said, we—government and the private sector—have learned a lot about information sharing in the past decade, and we must apply those insights to improve the future. The paramount lesson for both the government and private sector is fairly simple. Information sharing succeeds when it is targeted at solving specific problems and challenges. Information sharing is not an objective, it is a tool, and sharing for sharing's sake is not helpful. Threats and risks are not best managed by sharing *all* information with *all* parties, but rather by sharing the *right* information with the *right* parties (that is, parties who are positioned to take meaningful action). Targeted information sharing also better protects sensitive information (whether in the hands of the government or private sector), helps protect privacy, and actually permits more meaningful sharing of data.

Going forward, I believe that we must create two complementary information sharing capabilities, one focused on the most significant threats to national security and public safety, and another designed to enable greater automated management of IT security compliance across the federal enterprise.

The rise of the persistent and determined adversaries—whether or not state sponsored—poses ever-increasing risks. One does not need a security clearance to know that both the government and the private sector are suffering insidious and deeply damaging intrusions. Individually, organizations have visibility into only part of the problem and sometimes the damage may not be felt immediately (e.g., the harm caused by the loss of intellectual property may take time to materialize). We need new analytical approaches to tackle this pervasive threat that, if unchecked, could undermine our future economy, technology innovations, and perhaps even our national defense.

Such collaboration should be focused on the most significant threats to national security and public safety. The proposed National Center for Cybersecurity and Communications (NCCC) could, in part, provide this function and advance effective information sharing capabilities by:

- Exchanging technical data with rules and mechanisms that permit both sides to protect sensitive data;

- Analyzing the risks holistically (threats, vulnerabilities, and consequences) and developing strategies to manage those risks; and

- Developing cyber threat and risk analytics as a shared discipline.

For the NCCC to achieve success, the government needs to create the right legal environment for such information sharing and action and it must itself share information with the private sector.

In addition to increased information sharing about the most significant threats to the nation, we need to begin to address the adaptive cyber-security challenges facing both the public and private sector. Cyber-attacks can move at the speed of light or, with the right trade craft, they can unfold slowly over a protracted period of time. Through increased automation and real-time monitoring, we need to collect, analyze and disseminate information regarding attacks and develop better capabilities to respond quickly. Government and industry should collaborate so that this type of structured security automation can be used by all and, in certain circumstances, the resulting telemetry information should be shared or combined with similar data from other sources to provide a broader common view into patterns of exploit. Automation at its most basic level improves the security hygiene of an enterprise, but it can also be a foundation for sharing, analyzing, or possibly responding to potentially nationally significant events.

International Norms and Challenges

While a focus on good risk management and information sharing practices are critical, these efforts alone will not counter the global threat. We also need action internationally, and the government can help establish international norms in cyberspace.

The U.S. national security community, particularly the Departments of Defense and State, have a long history of addressing security norms in the context of nation states and military operations. In the Cold War, for example, the U.S. and Russia leveraged confidence-building measures to ensure that military exercises in one part of the world were not a precursor to a surprise invasion. In kinetic warfare, the existence of state action and the identity of the attacking state are relatively easy to determine. By contrast, cyber-attacks, even if launched against military targets, may be the work of non-state actors or individuals. The uncertainty due to lack of attribution complicates and confounds the legitimate ability of a state to respond.

U.S. foreign policy and diplomatic engagements on issues related to cyberspace security are not as focused as our efforts to combat terrorism or stem the proliferation of nuclear weapons. I believe that the U.S. must now marshal its significant diplomatic resources and expertise to advocate for cyberspace security and increase multilateral cooperation. Norms foster a shared understanding and common views that can bring a sense of order and predictability to nation-state conduct, serve as an effective way to mitigate the misunderstandings (and even conflicts) that can arise between states, and may establish ground rules for international cooperation that may help address non-nation-state actors.

I would caution that advocacy and cooperation are not goals in themselves. Like the discussion on information sharing, we need to focus advocacy and cooperation efforts toward specific outcomes. For example, working with like-minded nations to define clearly articulated norms of nation-state behavior in cyberspace could help to deter state support for cyber-attacks or hold nation-states that support such efforts accountable for their actions.

In the past year alone, the world has seen a surge in international dialogue around cyber-security norms. The dialogue has rapidly expanded from a focus on security norms, to include norms for privacy, freedom of expression, and access to the Internet. While broader dialogue and discussion on these additional topics is important, the security issues we face present somewhat unique concerns. As nations around the world continue to adopt and declare military doctrines for cyberspace, it is imperative that U.S. government focus advocacy and cooperation efforts toward specific and achievable short-term and long-term outcomes related to cyber-security.

The U.S. government should also insist that the private sector be integrated into these international discussions. Section 901 of the proposed legislation introduces some very important activities for the State Department to undertake, but it should also create a venue to integrate the views of the private sector into the formation of security norms. The private sector creates and delivers the technologies that nation states seemingly now want to exploit to promote their national interests. As a result, the private sector should be involved in domestic and international diplomatic efforts that are intended to curb attempts to militarize the information infrastructure that it designs, deploys, and manages.

Building a consensus on what constitutes acceptable behavior in cyberspace by nation-state actors, and building a partnership among those who view the functioning of these systems as essential to the national and collective interest, is a substantial national commitment. But the return on investment would be great. Developing a global understanding of norms of behavior in cyberspace is critical to the long-term stability, reliability, and security of the Internet and the critical infrastructures upon which we all rely.

Conclusion

At Microsoft, we recently celebrated the 10-year anniversary of Trustworthy Computing, an effort created for the express purpose of driving greater security, privacy, and reliability in our products and services, as well as fostering transparency into our business practices. During the past 10 years, we have developed numerous innovations, such as the Security Development Lifecycle, which reduces vulnerabilities in our products, and the Microsoft Security Response Center, which ensures that we can respond efficiently when new vulnerabilities or attack vectors are identified. These programs have had measureable, positive impacts on the security profile of our products and services.

During this time, the market greatly enabled U.S. leadership in cyberspace. The United States is home to many of the world’s most successful technology companies and one of the largest communities of Internet users in the world. But these market forces are changing dramatically and rapidly. Major emerging economic powers such as China and India are becoming centers of gravity for technology and innovation. Given that the United States will not have the same market forces at play in the future, the United States must seek other means to continue providing global leadership in cyber-security. I believe that what we have seen from Congress, in its extensive deliberations to craft a statutory response to cyber-security, provides a solid basis for continued U.S. leadership.