



"Cybersecurity: Threats to Communications Networks and Private Sector Responses"

**Statement of Robert B. Dix, Jr.
Vice President, Government Affairs and Critical Infrastructure Protection
Juniper Networks**

Hearing before the

**U.S. House Committee on Energy and Commerce
Subcommittee on Communications and Technology**

February 8, 2012

Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee, good morning. Thank you for inviting me to testify about cybersecurity threats to communications networks and private sector responses to those threats.

My name is Bob Dix and I serve as Vice President of Government Affairs and Critical Infrastructure Protection for Juniper Networks. Juniper Networks is a publicly-held private corporation headquartered in Sunnyvale, California, with offices and operations around the world. We deliver trusted, high-performance networking and security solutions that help public sector agencies, private enterprises, and service providers deploy networks that are open, scalable, simple, secure, and automated. Juniper's portfolio includes software, silicon, and systems for routing, switching, and security. U.S. Government customers (spanning civilian, military, and intelligence functions) rely on Juniper solutions for secure remote access, Network Access Control solutions for large agency enterprises, secure virtualization solutions for consolidated data centers and cloud computing, as well as mobility solutions.

Nature of Cybersecurity Threats

Despite its prevalence in our work, personal and everyday lives, at times we need to be reminded that the Internet was not engineered or built with security in mind. In fact, it has been only in recent years that security even has been included in the discussion along with performance, function, and reliability. Over time, the threats in cyber space have continued to evolve, and as we sit here today, the range of adversaries continues to expand. They continue to enhance their capabilities and their sophistication.

From script kiddies and hackers, to criminals and dissidents, to espionage and state-sponsored actors, the range of threat vectors is extensive. And let's not forget about the rogue insider.

The threats have evolved from viruses, worms, and trojans, to botnets, malware, and advanced persistent threats (APTs) that are pervasive. In fact, the ongoing theft of intellectual property may present one of the most serious threats to national and economic security.

Impact of Threats on Communications Networks

Information technology and communications networks are embedded in all manner of the nation's critical infrastructure, including power plants and the electrical grid, water filtration systems, financial systems, and transportation networks just to name a few.

While sector-wide risk assessments conducted or being conducted in the IT and communications sectors validate that networks are resilient, it is important to acknowledge that the risk continues to grow and change, and our efforts to protect and prevent must be sustained and agile.

In today's increasingly connected world, the move to cloud computing and the explosion in the use and proliferation of mobile devices and applications mean that we must be able to rely on the resilience of the network more than ever.

An intrusion into the network with a malicious payload can produce a significant disruptive impact with potentially serious functional, economic, and security ramifications.

Private Sector Response

In recognition of this reality, the private sector is working every day to protect against cyber threats through self-driven research and innovation, industry collaboration, and partnerships with government.

Information technology and communications companies invest significant budget and resources to drive the innovation and deliver solutions that will improve the protection, preparedness, and resilience of our public sector and private industry customers from the impact of cyber attacks.

As an example, Juniper Networks invests heavily in research and development into next generation networking and security solutions. In calendar year 2011 alone, Juniper spent more than \$1 billion on research and development.

This is but one example of the R&D investment made by a tech company. It is this type of investment that is driving much of the innovation that will change the world in terms of the way we communicate and operate in cyberspace. Collectively, we should be encouraging and enabling such investment and job creation.

In response to the growing cybersecurity challenge, the private sector has initiated myriad activities to address many dimensions of the various issues. Additionally, many companies and organizations in the private sector have committed resources, knowledge, expertise, and insight in working with our government colleagues through a range of public-private partnerships. Let me share just a few examples.

In 2007, a group of private sector companies came together to address the issue of software assurance and improving the development process and integrity of software and hardware products. SAFECODE (Software Assurance Forum for Excellence in Code) is a group of companies and subject matter experts that have set aside their competitive interests to gather and share industry best practices through a series of written deliverables that are available not just to the participating companies, but to the industry at large. SAFECODE has worked closely with the DHS Software Assurance Forum and others.

Additionally, in 2008, a group of private sector companies came together to address the need for collaborative, global incident response by forming ICASI (The Internet Consortium for Advancement of Security on the Internet). Once again, the participating companies, who compete vigorously in the marketplace, routinely share information in an effort to mitigate anomalous and abnormal network activity globally. Because the cause is greater than any one company.

Resulting from PPD-63 in 1998, which specifically addressed critical infrastructure protection and cybersecurity, and responding to a call for a public-private approach, the private sector formed Information Sharing and Analysis Centers (ISACs) across the private sector critical infrastructure community to enhance operational capabilities within and across sectors and their member companies.

At the request of the government, and concurrent with the development of the National Infrastructure Protection Plan (NIPP) in 2006, Sector Coordinating Councils (SCCs) were formed in the then 17 and now 18 critical infrastructure sectors to address policy and strategy issues

around risk assessment and risk management efforts to improve the protection, preparedness and resilience of our nation's critical infrastructure. These councils are self-organized and include participation across a broad range of companies, organizations and associations. They work closely in most sectors with their ISAC counterparts to include the operational component of the collaboration.

The Partnership for Critical Infrastructure Security (PCIS) is the coordinating body for the private sector critical infrastructure sectors and works closely with the Federal Senior Leadership Council under the NIPP Partnership Framework to advance the mission of critical infrastructure protection and cyber security. I should note that I serve as chairman for the PCIS. The partnership framework includes state and local government. Currently, the PCIS is working with the Administration on the implementation of PPD – 8 around National Preparedness; and the review and update of HSPD – 7 regarding an all hazards approach to critical infrastructure protection and cyber security.

Given that we cannot be truly successful unless we continue to advance the opportunities for collaboration between industry and government, and acknowledging that this is truly a shared responsibility, it is necessary to leverage all such opportunities. Through advisory committees such as the President's National Security & Telecommunications Advisory Committee and National Infrastructure Advisory Council, some of the great minds and technical experts in the world in government and the private sector come together to tackle hard challenges.

It is also important that we periodically test our preparedness and resilience through planned exercises. Over the past several years, industry and government have worked together to

design, plan, and execute the Cyber Storm series of Tier II national cyber exercises. This year, National Level Exercise 2012 will focus on cyber as a Tier I national exercise and presents an opportunity to test improvement actions implemented as a result of lessons learned from previous Cyber Storm exercises, as well as testing our national preparedness and resilience, including the current elements of the National Cyber Incident Response Plan and the National Cyber Risk Alert Level.

The information technology and communications sectors continue to innovate, making networks smarter and more resilient, looking to build more intelligence into the networks to protect the confidentiality, integrity, and availability of the data and to improve access and authentication controls to provide trust and security for online transactions and interactions.

Just a few weeks ago, a group of major Internet companies announced a voluntary initiative to prevent spam and phishing e-mails. PayPal, Yahoo, Microsoft, and Google are working on a new system to authenticate e-mail senders that will make it more difficult for bad actors to conduct their attacks through fraudulent e-mails.

These are just a few of the examples of productive efforts by the private sector to drive solutions, as well as evidence of the success that we can achieve when we work together in a truly collaborative manner.

Going Forward

Mr. Chairman, the number of users connecting to the Internet and other networks will continue to grow. Global Internet traffic is increasing at a rate of 40-50 percent per year. There are now

almost two billion Internet users and that number is expected to grow to four billion by 2013. It is also important to remember that the risk in cyberspace is dynamic. Threats and vulnerabilities evolve rapidly and the capability to manage and mitigate risk depends on an ability to be and remain agile and able to react quickly.

The technology and types of devices will continue to evolve and applications will continue to be delivered into the marketplace at a frenetic pace. The volume of data and video is growing exponentially and the demand for capacity, scale, and security will be paramount. The world of computing, storage, and networking is rapidly changing and evolving to meet those demands and security must be imbedded in the technology, the strategy, and the policy going forward.

The explosion in the use of smart phones and tablets and the advent and growth in the use of social media is rapidly changing the workplace and how we communicate, while introducing cyber risks in ways that few of us could have imagined only a brief time ago.

This is the *essence* of technology. It enables us to do to what we never imagined – and that includes those of us with nefarious motives. The convenience of technology has changed banking, purchasing and the sharing of personal financial information.

It is imperative that all of us acknowledge that cybersecurity is truly a shared responsibility, and that managing risk will require a true collaborative approach between government and the private sector. The private sector owns and drives the majority of the innovation, and also owns and operates the majority of our nation's critical infrastructure. The private sector also has access to important information that is relevant to the government, while the government has

access to much threat intelligence information that would be valuable to the private sector in advancing risk management activities to protect the network and the data.

We have the opportunity to seize this moment in time to build on the Comprehensive National Cybersecurity Initiative; the Cyberspace Policy Review; the National Strategy for Trusted Identities in Cyberspace; and many other efforts to improve the national and economic security of our nation.

The conversation about cybersecurity must include a discussion about the economics. But there are two sides to this coin. If we focus only on technology and technology development, we are likely to miss the opportunity to examine the challenges and impediments to technology and solution *adoption*. The market is delivering innovation at an unprecedented pace in history. However, the evidence would suggest that adoption of available solutions has not kept pace and should be a topic of further examination and discussion. Perhaps the business case or value proposition for investment has not been adequately communicated to user constituencies of all levels, from home users, to small business, to academic and non-profit institutions and even to large enterprises.

Many low cost and no cost solutions are available to improve any user's protection profile. Incentives for businesses such as liability protection, market recognition and differentiation, and even tax incentives may spur investment in an advanced cycle.

Accordingly, there are many things that we can do together. It is reported by reliable sources that some 80 percent of exploitable vulnerabilities are the result of poor or no basic cyber

hygiene.¹ For me, this is basic blocking and tackling. If we can raise that bar of protection, it makes it more difficult and more costly for the bad guys do harm.

When our nation was confronted a couple of years ago with the threat of the H1N1 virus, we mobilized as a nation to warn and advise folks how to protect themselves from the risk of infection. We all remember the messages, public service announcements, posters, radio, TV, and Internet messages regarding the need to cough into our sleeves, wash our hands, and other protective measures to secure our health. The effort included the CDC, HHS, and other federal departments and agencies, along with many non-profits, businesses, and organizations.

We have the opportunity to use the same model for a sustained awareness program to help educate citizens, small businesses, students, non-profits and other stakeholders on how to protect themselves from the risk of malware, phishing and other forms of infection in cyberspace.

Many federal departments and agencies interact with citizens and businesses routinely. Leveraging the Small Business Administration; the Internal Revenue Service; the U.S. Postal Service; the U.S. Department of Education; and others would provide an ability to scale the messaging across a wide range of the population. Perhaps we could even convince every Member of Congress to include a link on their constituent website that directs folks to where they can get more information about protecting their health in cyberspace.

¹ See CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY IN CYBERSPACE, HEARING BEFORE THE U.S. SENATE COMM. ON THE JUDICIARY SUBCOMM. ON TERRORISM AND HOMELAND SECURITY 111th Cong., 2d Sess. 19 (Nov. 17, 2009) (statement of Mr. Richard C. Schaeffer, Jr., Director, Information Assurance Directorate, National Security Agency).

We should be proactively enlisting the expertise and innovation of telecommunications service providers and content providers to engage in the path forward. Many are already engaging in innovative efforts to identify and notify consumers about infections.

Many of you on the Subcommittee and Full Committee have been actively involved in attempting to address the issue of facilitating the exchange of intelligence information and creating a true partnership between government and industry to build enhanced situational awareness to improve detection, prevention, and mitigation of cyber events that may become incidents of national consequence.

Though the private sector is doing work internally to address the threat, the government has an important opportunity to do a better job of providing threat indicators and intelligence to private industry. Far too often, government continues to compartmentalize and restrict access to relevant information. In order for private industry to be able to prevent and mitigate threats, industry must have access to the threat information that the government possesses. Keep in mind, this does not mean industry needs access to sources and methods – rather, access to information about Tactics, Techniques, and Procedures will improve the ability to manage risk, acknowledging that we simply cannot protect everything all the time...just as is true in the physical world.

With this in mind, legislation introduced by a Member of this Subcommittee, Rep. Mike Rogers (R-MI), in his capacity as Chair of the Permanent Select Committee on Intelligence, H.R. 3523, the “Cyber Intelligence Sharing and Protection Act of 2011,” would amend the National Security Act to facilitate the sharing of cyber threat intelligence with eligible private sector entities.

Wisely, the bill protects the sensitive nature of such information by requiring that security clearances be granted as necessary to the relevant private sector entities. In addition, the bill ensures that the private sector treats the sensitive information as such – private sector recipients of the threat information may use it only to protect rights and property. Finally, the bill confers liability protection for companies that choose to protect their networks or share information based on the authorities provided under the bill.

This legislation will add an arrow to the protection quiver by addressing a key impediment to building cyber situational awareness.

Through the development of the National Cyber Incident Response Plan, and many other examples, we have proven time after time that when we work together, the results are more productive.

Accordingly, going forward we need to work together to map the gaps in technology as well as legal and policy impediments to improving our cyber security posture. Building on the current efforts to conduct risk assessments and risk management plans in each sector through the Sector Coordinating Councils, we can work to refine high probability, high impact risk; the recommended protective measures; and potential gaps that would be candidates for research and development activities, either in the private sector or government. Working together, we can continue to collaborate with the National Institute of Standards and Technology (NIST) and other standards bodies to develop and update recommended security provisions to enhance overall risk management.

Conclusion

Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee, we must move beyond just thinking about the challenges of today...to thinking about the risk profile of tomorrow. Today's cyber attacks are more complex and often difficult to detect, and can target classes of users – even specific users – gaining access to valuable data and causing significant harm.

We have an opportunity to operationalize information sharing, analysis, and collaboration to build true situational awareness and an enhanced common operating view of the cyber domain to improve detection, prevention, and mitigation.

We need to continue to examine opportunities for developing a cyber savvy workforce and overall population.

With a commitment to working together in a collaborative manner, the United States will lead the effort to improve the protection, preparedness, and resilience of critical infrastructure and cyber security.

On behalf of my colleagues in the industry and the more than 9,000 proud employees of Juniper, I thank you again for this opportunity to testify on cybersecurity as it relates to communications networks. The threat is real...the vulnerabilities are extensive...and the time for action is now. The American people are counting on us to get this right. And the private sector looks forward to continuing the collaborative relationship between Congress, the Administration, and private industry on this important issue.