SENIOR LEADER PERSPECTIVE: ROBERT DIX, JR.

NSCI's Lindsay Trimble recently interviewed Robert Dix, Jr., vice president of government affairs and critical infrastructure protection at Juniper Network, Inc. Dix has served in senior executive positions in the information technology sector, as well as appointed and elected positions in the public sector. Among his various roles with Juniper, Dix serves on the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee and represents Juniper as Chair of the Cyber Security Collaboration Task Force. He served as Chairman of the IT Sector Coordinating Council from April 2008 until January 2010 and continues to serve on the Executive Committee. In that role, Dix is also active with the Partnership for Critical Infrastructure Security, where he is a member of the Executive Committee and serves as liaison to the National Exercise Program. During the 108th Congress, he served as the Staff Director for the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Dix was honored with the prestigious Federal 100 award in 2008 and 2010.
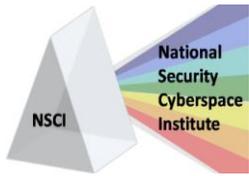
You are a part of a number of organizations that focus on public-private cooperation to improve cybersecurity and protect our national critical infrastructure. Can you give us any specific examples of information sharing that is occurring between public and private organizations?

First I should note that "information sharing" just for the sake of sharing information is not what we're trying to achieve here. But, let me touch on the specific answer for a moment.

HSPD-7 required the creation of a plan to protect the nation's critical infrastructure and that produced something called the National Infrastructure Protection Plan (NIPP) released in 2006. Among other things, the NIPP set the framework to establish Sector Coordinating Councils and Government Coordinating Councils in each of the then 17 – now 18 – critical infrastructure sectors. Since 2006, in my sector – the Information Technology Sector – and also in the Communication Sector, we established coordinating councils and have been very active in that collaboration with government over time.

Let me give you an example of information sharing that has produced a positive result. One of our charges for the IT Sector Coordinating Council was to conduct a risk assessment of our sector. We decided that for information technology, it really wasn't about protecting assets. It was really more about the functions we deliver that are interdependent and that all sectors rely on to accomplish their own mission critical activities. We set out to create a risk assessment based on critical functions and we completed that; it was released in August 2009. More than 80 subject matter experts from industry and government worked together on issues such as domain name services; products and services; incident management; etc. We used an Attack Tree methodology to complete that risk assessment. That has been well received and we're already working on version 2.0. What the baseline risk assessment

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **Page | 1**

achieves is a comprehensive examination of threats, vulnerabilities and consequences and tries to identify the high-likelihood and high impact threat and consequence areas that we need to address; develop protective measures; and inform recommendations around research and development. We're now looking to a process of implementing a plan for risk management and building a set of metrics to help us have a better idea if what we're doing is actually achieving the outcomes we desire.

It has been a very collaborative process where representatives from the private and public sector have really rolled up our sleeves and shared information with the various stakeholders to create an accurate risk assessment of the information technology sector.
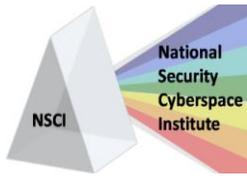
A second example is Information Sharing and Analysis Centers or ISACs. There are 13 of them in various sectors; those are our operational partners. So the Sector Coordinating Councils work on policy and strategy and the ISACs are more focused on the operational component. We have a very effective IT ISAC that has a 24/7 watch-and-warning capability that helps issue alerts, warnings and information about protective measures. They work very closely with USCERT and other elements of the government to collaborate on events that may require attention. It's an industry organization that collaborates effectively in industry and the government space.

Lastly is the Comprehensive National Cyber Initiative or CNCI. One of the elements of that, which we affectionately refer to as "Project 12," looks at public-private partnerships and information sharing – the partnership framework, the partnership model and how it enables information sharing. During implementation of the Project 12 recommendations, we have launched – and will launch – a number of pilot projects that actually identify what information is of value that we could share from industry to government and from government to industry. That process has been going on since the end of 2008.

From your perspective, why aren't we doing better at this? Funding? Technology? Shareholder confidence regarding private companies?

I would say that it's all about people, processes and technology. On the "people" side of the equation, there are cultural issues. We still live in a world that has a huge focus on the "Cold-War mentality" of the "need-to-know" regarding information sharing. With the threat climate that we have, the challenges we have and the critical infrastructure protection and interdependencies associated with those, it is absolutely a necessity that we move to a "need-to-share" approach. This is vital to how we address national security, economic security and the collaboration between industry and government. I recognize that there are some things the government does that need to remain within government and there are some things in industry that need to stay within industry, but there are a lot of things we can do better, in terms of changing the culture to recognize the value of collaboration.

The "process " piece of it goes along with that. We have policies and regulations that are outdated and sometimes we want the ability to be more collaborative.

110 Royal Aberdeen ⚫ Smithfield, VA 23430 ⚫ ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 2**

We've actually done a good job at the "technology" part of it. Although the market has delivered some very good collaboration tools and capabilities, we find that they are just terribly underutilized. This is less a technology issue, and more of a cultural one – back to the "people."

We are trying to drive forward on that with the understanding that our national and economic security relies on it.

What do you see as the similarities and differences between public / private cooperation challenges and challenges with interagency and international stakeholders?

Some are the same; some are different. As you know, many U.S. companies are multinational/global, so that creates some challenges right there, in terms of the collaborative piece of it. Again, we are working through those issues and challenges to try to improve the model that allows us to be better at this.

In terms of the interagency challenges, we continue to see that progress there is often slow. Many of us in industry feel that this issue of cybersecurity is such a high priority, that we need to identify a plan, a set of actions and milestones and we need to get to it. That's not typically the way government works, and there are many long-standing reasons for that. But we need to understand and recognize the consequences of not moving faster to improve on some of this.

When we get to the international component, the governments' models for information sharing are different; the cultural attitudes about some of these issues are different. We all want to be able to respect privacy and civil liberties; that's a fundamental part of what we want to do. That's a big focus in cyber. There's sometimes a challenging balance around all of this. But what are the policies of our respective governments and where can we find common ground?

There are many different challenges and we have to try to stay on top. I think the United States can do better at participating with international bodies in policy-making and standard-setting. In many ways, we're taking steps to do that. In the past, we haven't been nearly as good as we need to be from a participatory standpoint, but I believe we're taking steps to improve upon that.

What are some "best practices" you've seen that other organizations and/or nations could adopt to improve cybersecurity information sharing and collaboration?

This is breaking new ground in many cases. We have been unsuccessful until very recently at having a clear understanding of what it is that we need to share; what we have that would be of value; and what the impediments to that would be. We're still trying to get our act together here.

So, what are some of the models and best practices? We're seeing some of those examples in existing bodies. In the United States, the National Coordinating Center for Telecommunications and the United States Computer Emergency Readiness Team (USCERT) both have an international component. When you're dealing with emergencies, such as what's currently going on in Haiti, we do collaborate internationally with our partners to address what those challenges and needs might be and to share information.

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **Page | 3**

There are places that we can continue to build, get better and learn. Law enforcement is a place where we're trying to improve our information sharing. There's got to be improvements on how we work together from a law enforcement standpoint. A lot of cybersecurity challenge is driven by the criminal element, so we have to understand how we need to work better together across the various communities to address the criminal law enforcement pieces of this as well.
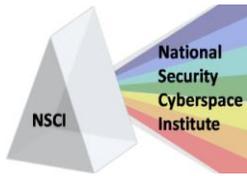
Supply Chain Integrity has also been highlighted as a key area impacting cybersecurity. Routers are obviously a key component of network security. How has Juniper Networks approached this challenge?

We're very proud of what we call our Brand Integrity Program. We have a holistic approach to supply chain risk management – from concept to delivery, whether it's hardware or software. We have a very rigorous audit and inspection process in place that vets the resource piece of it; our suppliers and partners, as well as our customers; and what happens with our products as they move through the supply chain. It is very robust and very comprehensive.

We do background checks on potential partners and suppliers. There are a lot of things we do throughout that entire program that try to reduce the risk of either counterfeit products or other penetrations into our supply chain that may be of a nefarious nature.

We're very proud of that and we've been working with the government, our colleagues in industry and others to try to educate them about supply chain security. We, at Juniper, are a member of an organization called the Software Assurance Forum for Excellence in Code –SAFECode – an industry-driven, international collaboration looking to improve software assurance. One of the issues that we have addressed with a white paper is that of software and hardware integrity; and supply chain security is clearly a part of that. As a community, we're looking at this as well. We're working with the government through NIST; the Department of Defense; the Department of Homeland Security; and we also have substantial industry participation.

From our standpoint at Juniper, we're trying to take our best practices and lessons learned and share them with our colleagues in industry and with our friends in government. I'd like to share something I've learned in being very active in the dialogue around supply chain risk management and its threat to national security. One thing industry is asking is that the government take a look at its own acquisition procedures. In other words, the government still has a tendency to buy based on low price, so they will shop online at product broker sites looking to get the lowest price. These are not authorized resellers of our products and sometimes they deliver defective or even counterfeit equipment. We even know of some people that may have ill-intent penetrating the supply chain through eBay. The United States government has, in the past, made purchases off of eBay. It's pretty easy to put nasty things into the supply chain through eBay and other unauthorized online brokers that are sometimes involved in nefarious online activities. I describe that as a "low-hanging fruit" part of the solution. It seems to me that should be something that could be corrected fairly easily with a policy declaration – "We're not

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro *Improving the Future of Cyberspace...Issues, Ideas, Answers* **Page | 4**

going to do that anymore." The government should buy only from authorized manufacturers, distributors and resellers.

We're all in this together and we all have ways that we can continue to improve our processes to ensure the integrity of those processes in the outcomes.

During a time of tight budgets, how are the organizations you represent and task forces you participate in enhancing security measures and pushing ahead for innovative cybersecurity solutions?
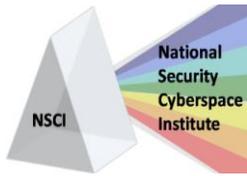
Industry is still investing in innovation – at Juniper, investing in Research and Development remains a high priority. We all recognize that there have been economic challenges. I'm a big believer in the free-enterprise system and that the market delivers solutions to the challenges that we face. Industry is still making investments in research and development and in innovation. We are constantly looking at getting ahead in this situation.

We, at Juniper, are also involved with our industry partners and with government in various activities, looking at how we're going to be able to deliver communication capabilities in the "future Internet," as I'll call it. As we know, we're operating on an Internet that wasn't exactly built for the scale at which we now use it, nor was it built with security in mind to deal with some of the characters that operate in cyberspace. Many of us in industry are actively engaged with the government on a research and development agenda. We're also looking outward to find what it's going to require with next-generation networks and how we're going to change it, particularly as we work in the wireless realm and more people are relying on these devices for connectivity. That's going to continue to be a challenge.

Even in times of tough economic issues, we're still actively engaged in looking ahead to the future and being involved in the dialogue to find solutions around things such as virtualization; cloud computing; federated identity management; and ways that we can reduce our space, power and weight in order to be more "green" in ways that we deliver solutions to the marketplace. It's very exciting to be in an industry that is so driven by innovation and is regularly delivering exciting new solutions to the marketplace to address these challenges.

Many organizations continue to spend significant amounts of money on after-the-fact network defense (e.g. anti-virus / signature-based mechanisms). Can you tell us a little bit about how we, as a nation, can get out in front of the threat via active defenses?

I really appreciate the question and believe there are a couple pieces to the answer. First, on the government side, there's the Trusted Internet Connection or TIC initiative, led by the Office of Management and Budget [OMB] to optimize individual external connections, including internet points of presence currently in use by the federal government. This common solution is designed to facilitate the reduction of the federal government's external connections to the Internet. Reducing your exposure is clearly an effective means of keeping out the bad guys, provided you can still conduct agency business effectively.

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 5**

At a more fundamental level, we – as a nation, as consumers and companies of all sizes – have to improve our overall basic "cybersecurity hygiene." President Obama spoke of this issue with the release of his Cyberspace Policy Review in May, as being a priority. In many cases, we have people operating computers who don't understand anti-virus and updating signatures; they don't understand firewalls; they don't even understand password management. They don't understand some of these elements that are basic fundamental parts of cybersecurity hygiene. In industry, there are a lot of places where we can do a better job across the spectrum, including the process of patch management.

In my opinion, we need to have a campaign focusing on fundamental cybersecurity hygiene. We need to bring together a tiger team of smart people in industry, academia and government and agree on the top six, eight or ten fundamental elements of best practices around cyber hygiene, then have a national awareness and education campaign. Small businesses typically don't have IT staffs, but there are still things they can do that don't cost a lot of money that help protect their operations and, in doing that, protect the nation.

One of the biggest attack vectors is through botnets – computers that are taken over by someone else, through an exploitable vulnerability. Potentially, those vulnerabilities can be reduced if we improve our hygiene. According to research, approximately 80 percent of the exploited vulnerabilities could be mitigated if, across the board, we did a better job of improving cybersecurity hygiene. That's striking! To think that, through such fundamental best practices, we could reduce the surface of exploitable vulnerabilities by such a large percentage – or even close to that percentage – is striking.

Improved cyber hygiene helps us all in this effort. We know what these best practices are, but we have to get people to understand them. Utilizing Internet service providers is part of the solution, but we also need to utilize the Small Business Administration; they have contact with small businesses all across America. How about the Internal Revenue Service? They have contact with individuals and businesses across the country. How about the U.S. Postal Service?

We are all in this together, so we need to have a collaborative approach to dealing with a national education and awareness campaign focusing on improving cyber hygiene. By the way, President Obama has talked about that in his 60-day cyberspace policy review as being a priority. If we raise that bar, we can make it harder for the bad guys. That should be part of our overall national strategy.

What are the major challenges to doing this?

Getting it done – that's the biggest thing. Somebody needs to lead. I'm hoping that the White House will follow through as they have on many other initiatives. The previous administration and this administration have provided additional leadership to get this type of national campaign going, bring people together and help them understand the cyber hygiene piece of it.

We need to help people better understand that everybody has stake in this. A lot of users are not tech-savvy, so we need the participation of all the people who have the ability to share with folks. Industry is already responding in a lot of ways by providing built-in security with products that are delivered into

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 6**

the marketplace, but there are ways that we can educate people in fundamental things they can do and ways they can protect themselves that would help raise the bar for everybody. That should be our objective.

This whole botnet thing is a crisis. We need to reduce the ability of bad guys to have access to and build and deploy those bot armies through the exploitable vulnerabilities that exist out there – while working to reduce those vulnerabilities as well.

**It seems like such a simple solution, doesn't it?**

If I were king for a day, then we'd get some messaging together, craft a series of public service announcements and at least get started. We had Cyber Security Awareness Month last October, but we need Cyber Security Awareness Day every day. That's going to take leadership at the national level, in Congress and in industry. By the way, industry is ready, willing and able to be a participant; we do it every day. Look how we reach out – from an education and training standpoint – to our employees and our customers. We need to, again, help people understand how to train and educate, and know what materials they need to help their employees understand cyber hygiene. That's a way that we can begin to build momentum and have people understand that we're all in this together and everyone is a stakeholder. Everyone.

There are some things that are happening in government and industry that have the chance to really make a difference in this subject. I previously mentioned the Trusted Internet Connection initiative. The Federal Desktop Core Configuration Project provides a standardized configuration across the federal enterprise – a required implementation for all federal agencies. In and of itself, that begins to reduce a number of these exploitable vulnerabilities. The Consensus Audit Guidelines, developed by a consortium of federal agencies and private organizations, and recently mapped to NIST guidelines, identifies the top 20 security controls, so that people understand where to prioritize their security efforts and their investment around those security controls. In auditing the process via continuous monitoring – we're moving away from simply a process compliance approach to one of active protection , measures and metrics to be able to determine our level of success.

I want to emphasize that there are things going on with industry and government working together to identify solutions. We are hoping many of these initiatives will continue to proliferate across the commercial sectors, as well as the public sectors, research and education communities. There are some very creative things going on that are producing results toward our shared responsibilities in cybersecurity, but they all need to integrated within a broader campaign.

You have participated in national level exercises, including CyberStorm. How are these impacting the security of our critical infrastructure?

There are two sets: the National Exercise Program, which is Congressionally-mandated and is driven by 15 different planning scenarios that are primarily physical-event based. There's also the CyberStorm
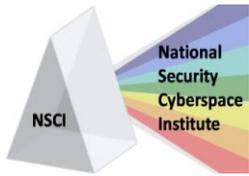
Series, which is a Tier II exercise program focused primarily around cyber. There have been two of them already and there will be a third later this year. I participate in both of those.
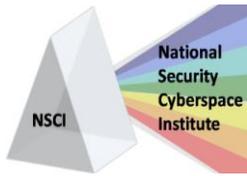
These are about testing our preparedness and resiliency. We have lots of plans as to how to deal with natural disasters, terrorist attacks or other kinds of events, but we need to talk more about the convergence of physical events and cyber events. A physical event, such as a hurricane, flood or wildfire, has cyber consequences and those need to be considered. A cyber event may have physical consequences, for example if there's an outage in the power grid or some other control system that can affect pipelines, water supply systems, etc. We need to look at this from an all-hazards approach and test our national preparedness and resiliency. We should not be afraid to learn that we might have some significant gaps. The whole idea of conducting exercises is to learn and get better.

Past exercises, in some cases, have been more bureaucratic and about "checking the box" rather than being honest about where the gaps are in our preparedness and resiliency. We need to move more in that direction. Until very recently, the private sector and specifically the owners and operators of our national critical infrastructure have not been invited to be a part of the process in any significant way, but that's changing. As we sit here today, I am privileged to chair the National Private Sector Working Group for National Level Exercise 10 and 11. We're working to integrate the owners and operators of our critical infrastructure into NLE 10 and NLE 11. This is a pretty dramatic change and is a result of our tenacity to try to have our friends in government understand that the private sector owns, operates or controls the prevailing maturity of this nation's critical infrastructure and that today's interdependencies are critical. When we test our preparedness and resiliency, we need to be at the table and be fully involved and engaged. When a real-life event happens, they need us and we need each other.

CyberStorm 3, later this year, will give us an opportunity to test the lessons learned in CyberStorm 1 and 2 and test elements of the National Cyber Incident Response Plan, which is under construct. That was one of those action items coming out of the president's 60-day cyberspace policy review. Industry is very much engaged in CyberStorm 3 – in the design, planning and execution of the exercise. There are many good things happening. We just need to be sure we test with as much realism as possible and are willing to accept the fact that there may be gaps – in some case, significant gaps – and that we should address lessons learned as part of our continuous improvement around preparedness and resiliency.

What do you think about states and local communities conducting similar exercises, obviously on a smaller scale, to improve their processes and capabilities to defend against and/or operate through cyber-related incidents?

That's happening in both cases. National Level Exercise 11 includes participation by 4 FEMA regions, 8 states and many local governments. CyberStorm currently has 10 states involved as well as some of our international allies. I believe there is a great recognition that we must integrate these activities to include our friends in state and local government and, to the extent possible, our international partners. That's a great part of this process. When something happens, all things are local, right? We need to understand how all the pieces fit together and address the issues of access security and fuel. That's a big

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 8**

part of testing our preparedness, so the state and local governments are key partners and key stakeholders in these national-level exercises.

It is no secret the bulk of government cyber infrastructure is actually owned and/or managed by private industry. What are some ways you think government can incentivize private industry to better secure this infrastructure?

We have taken a look at the whole issue of incentives. We recognize that oftentimes the government has the tendency to take more of a stick approach to solving issues. Industry typically believes in a more reasoned approach with a potential combination of sticks and carrots to drive change. An example of this would be liability protection and a "safe harbor" for those that are actually trying to do the right thing. There are a number of other incentives, such as potential tax credits – a tough sell in this current tough economic climate – but there is a whole series of incentives that we collaborated with our friends in government to produce for consideration. Here's a sample of what we came up with:
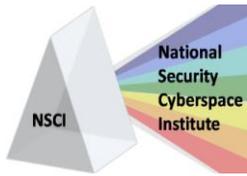
- Liability reform
- Tax credits
- Grants for research & development
- Small business grants
- Malcolm Baldridge-type awards for cyber excellence

Some people have called for a national capability to detect "bugs" that serve as entry points to cyber criminals and hacktivists. What are your feelings on this?

This goes back to the issue of cyber hygiene. We talked about potential exploitable vulnerabilities. There will never be a product that doesn't have a potential defect. Industry has been working to minimize any defects that may be exploitable vulnerabilities through enhanced software and hardware assurance and integrity programs, training and education, and comprehensive system development life cycle integrity programs

Is there anything else you'd like to add?

Another capability that I believe is absolutely essential, particularly in cyber, is that as we sit today, we don't have a joint integrated public-private 24/7 operational capability that focuses on detection, prevention, mitigation and response to cyber events that may become incidents of national significance. Some of us in industry and government – primarily industry – have worked to put a framework together that we believe would move us in that direction, in an effort to enhance situational awareness and build a common operating view in the cyber domain, during steady state as well as crisis conditions. This might help us improve our chances at getting ahead of events, rather than keeping our energy in a responsive or reactive mode. We can improve the way we share information between industry and government, industry and industry and government and government, around threats, vulnerabilities, anomalies and abnormalities that are happening on the networks better than we do today.

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *Improving the Future of Cyberspace...Issues, Ideas, Answers*   **P a g e | 9**

In industry, we're doing a reasonable job at this within sectors, but we can do a better job across sectors and we must be able to do a better job with government. That circles me back to what I said earlier about a "need-to-know" culture versus a "need-to-share" culture. We must have the ability to have a command center or a national preparedness coordination center that allows us to have trusted subject-matter experts from industry and government working side-by-side and/or virtually to understand what's going on in cyberspace, so that when we see something that looks unusual, we share that with one another in an effort to try and develop protective measures to mitigate rather than always being in a position of reaction or response.