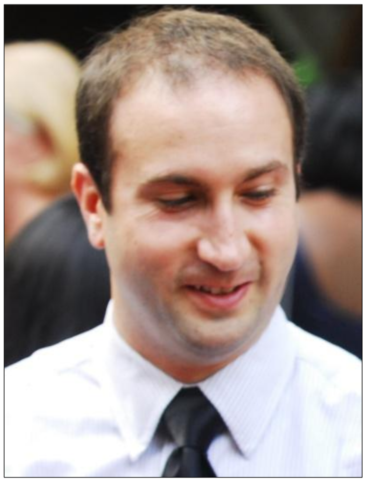
National Security Cyberspace Institute NSCI

CyberPro

August 2010

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: CYBER SUPPLY CHAIN



Hart Rossman

NSCI's Lindsay Trimble recently had the opportunity to discuss the cyber supply chain with Dr. Sandor Boyson, research professor at the University of Maryland Robert H. Smith School of Business, and Hart Rossman, vice president and chief technology officer for Cyber Security Solutions at SAIC. Rossman is a senior research fellow with the University of Maryland's Supply Chain Management Center, where Boyson serves as the founding co-director.

Dr. Sandor Boyson

As defined in their joint white paper published in June, the cyber supply chain is "the mass of IT systems – hardware, software, public and classified networks – that together enable the uninterrupted operations" of government agencies, public companies and their major suppliers. "The cyber supply chain includes the entire set of key actors and their organizational and process-level interactions that plan, build, manage, maintain, and defend this infrastructure."

NSCI: Would you give us a little background on the research your team has done on the cyber supply chain?

BOYSON: I am co-director of the University of Maryland's Business School's supply chain management center and my background is both with the IT and business aspects of supply chain. I also served as the chief information officer for the Business School and built out technological infrastructure that we use globally. In that role, I had the opportunity to understand some of the enterprise architectures and key components of fielding complete IT systems, particularly global portal systems.

We've also built portals that demonstrate very high degrees of interoperability and openness for clients, such as the Department of Defense. We built a major supply chain portal demonstrator for the Office of Secretary of Defense in 2000-2001; this was for the Air Force's F101 Engine/B1 Bomber supply chain. We built the second one in 2004 for the Army's HIMARS missile launcher system in collaboration with Lockheed. These portals brought together all of the key actors across a system's supply chain in a real-time environment that displayed the role-based views they needed to do their business. The portal was based on a very secure LDAP environment. The users would come in, be recognized, have certain permissions and be able to access – based on these permissions – whatever functionality they were required to have for their work.

It was a very interesting experience putting those portals together. We began to understand in a much more detailed way what it would take to secure a widely distributed group of actors globally.

Going deeper into some fundamentals, our research over a decade has continually pointed out the need for businesses to overcome stovepipes. In the mid-'90s, we did studies for the Department of Energy and various players in DoD about what were best practices in the supply chain. We found out that, consistently across the 1,600 companies we surveyed or interviewed, they were struggling to overcome functional stovepipes and work as cross-functional supply chain teams – not only across their own enterprises, but with their partners worldwide. The vanguard companies were forming these extended global supply chain teams supported by real-time technology. The technology enabled these teams to achieve a tremendous amount of time and process compression. Importantly, demand signals coming from the customer base were rayed out simultaneously to all key participants in the supply chain. This is crucial because the supply chain is really about a group of companies working together as a business ecosystem that can serve a common customer base with a product or service. That's really the goal of the supply chain.

We've released two books based on our prior research. The first book, "Logistics & The Extended Enterprise," looked at process integration within and between enterprises sharing a common supply chain. We found, for example, a number of companies had appointed vice presidents of the supply chain and were linking procurement, distribution, manufacturing and supplier management under one centralized, highly-empowered chief supply chain officer position. In 1996-1997, about half of Fortune 500 companies had such a position in place.

Our second book, "In Real Time: Managing The New Supply Chain," looked at how, once the kind of coherent managerial governance structure described above came into being, it enabled companies to look across entire supply chains and decide what to keep inside and what to outsource. I'm talking about the governance – the strategic management – of highly-distributed activities across the supply chain, some of which are done internally and some of which are outsourced, but all of which are coordinated. There was a lot of visibility and information sharing across this entire chain based on technology – sharing a common portal, for example.

Since then, several things have happened – 9/11, Hurricane Katrina, global economic meltdown. What we were seeing in the private sector and began studying intensively five years ago is the concept of formal risk management applied to the supply chain. How do you balance risk-and-reward across a highly-distributed supply chain? For example, does it make sense to maintain a highly-outsourced supply chain or is the risk of disruption too high? What *is* the right balance? What is the right governance structure to manage accelerating risk across the global supply chain?

We started to see the emergence in industry of chief supply chain risk officers. Their chief responsibility is to manage the risks that might disrupt operations. For example, there's a group of suppliers located in an earthquake zone. Do you need alternative suppliers lined up, so that if something happens to your critical suppliers you have some means of maintaining business continuity? To address these contingencies, we began to see the emergence of a sophisticated, analytics-driven executive function called the chief supply chain risk officer.

We have a new book coming out this month: “X-SCM: The New Science of X-Treme Supply Chain Management.” This book has 16 co-authors that we believe have done some of the deepest thinking and have the most practice experience in this area. One of the co-authors is John O’Connor from Cisco, who manages the risk function of the supply chain for Cisco and has created a highly-sophisticated operation that extends from product design all the way through the actual distribution of the product to customers.

So I’ve described the big picture of the evolution of supply chain management as an emerging discipline that first worked to unite real, physical processes and distributed actors in the product supply chain in the early ‘90s. This internal and external integration unfolded among groups of companies that worked in product supply chains and the emphasis shifted – once these global supply chains were up and running and exposed to a lot of risk – to monitor and manage risk.

That leaves us with the cyber supply chain. Hart Rossman is the chief cyber technology officer for SAIC. He raised the issue of whether these kinds of supply chain insights can be employed in the cybersecurity realm. We began to understand that there needed to be a lot of fundamental research questions asked and addressed in order to understand whether or not supply chain risk management as a discipline could be applied to cybersecurity systems.

So, with support from SAIC, we began to have series of developmental activities and research. We interviewed approximately 30 national cybersecurity experts that represented different parts of what we defined as the cyber supply chain. By defining the cyber supply chain, you have to overcome the functional stovepipes that are really hurting cybersecurity right now. What I mean by that is the software community, the hardware community, the network provider community and the systems integrators who bundle together these elements into an operating system. It also includes policy people and acquisition specialists, who work at the corporate level to define systems requirements for the integrators.

Again, these players are all a part of a *living* cyber supply chain. The problem is they don’t work across the chain. They work inside their own realms or disciplines. So the software community is looking for common vulnerabilities. The hardware community is looking for counterfeit products. Network operators are looking for anything that could diminish or deteriorate the availability of the network or cut down the speed of the network. Integrators are looking for anything that could knock a project off schedule.

Each of these actors is a key player in this collective, global supply chain. It’s global because in each of these domains – whether it is hardware outsourced to companies in Indonesia or Thailand, software outsourced in India or China, or network management services outsourced to third party network providers or cloud service providers – there’s a tremendous globalization of sourcing.

In the meantime, policy and acquisition people need high levels of total systems assurance around confidentiality and ability to defend against attack. And they are starting to demand that supply chains act like supply chains – with conscious collective risk management leadership.

But, the IT supply chain stubbornly does not regard itself as a coherent supply chain. It regards itself as a series of discreet, separate disciplines and domains that produce inputs that then get passed on to the next player in the chain. There is very limited coordination between all of these players. That lack of systemic management of the IT supply chain prevents software, hardware, network provider and system integrator from collaborating in an ongoing way to identify risks to the host system and gaining visibility over end-to-end operations. This lack of visibility and strategic control is a major detriment in preserving cybersecurity. There are too many blind spots.

NSCI: Thanks for that overview, Dr. Boyson. Mr. Rossman, with the cyber supply chain, security experts must think about the security of their internal networks as well as security along the way – from product assembly to delivery. How do we ensure the integrity of hardware and software to limit cyber security vulnerabilities before they happen instead of being reactive and trying to patch issues after the fact?

ROSSMAN: As Dr. Boyson pointed out, the first thing we have to do is move beyond the stovepipes in individual enterprises and organizations from two perspectives. The first is to understand that, in all likelihood, the organization that is buying whatever product, service or solution is currently being discussed is not really the terminus for that product. In other words, they're going to acquire it in order to provide some service, product or solution downstream into their customer base. So we can't just focus on securing the upstream supply chain, but we also have to be able to forward-integrate the assurance measures into our own customer base because in all likelihood, whatever service, solution or product we provide to our customer, they're going to incorporate some sort of offering and provide that to their customer downstream. So we have to recognize that we have to get out of these enterprise stovepipes and not just focus upstream in the supply chain, but be able to forward-integrate assurance measures.

I think the way we do that is by looking at the interrelationship between system development or product development lifecycles across the supply chain; looking at those touch points; and looking at opportunities to gain greater visibility and awareness into what's occurring and make the right risk-based decisions on how to identify the threats and mitigate them as we hand off products, services and solutions – or the components that comprise them – as we move down the supply chain into the customer base.

NSCI: In software, there is an average of 2 to 46 errors per 1,000 lines of code for good programmers. How do we test for errors we don't even know exist?

ROSSMAN: If I can turn the question around a little bit, it's obviously always difficult to prove a negative and it's hard to know what we don't know at a very specific level. What we *can* begin to do is broaden our quality assurance and our compliance testing and evaluation procedures to look beyond technical things we would usually look at.

For example, we're exclusively talking about software. One of the things I'd like to see over time is for us to take a more holistic view of testing across the supply chain and be able to look at software vulnerabilities and user apps – programs or applications the user might encounter – in relationship to software vulnerabilities and firmware – the low-level software that drives the hardware – and look at that in relationship to how we're testing and debugging the hardware. Taking a much more holistic view is important. It will never completely tell us what we don't know, but it gives us a better picture of what the quality of the entire product looks like. What we're ultimately trying to boil it down to is a common operating picture for threat, vulnerability and quality across the supply chain, rather than looking at it individually as just software, firmware or hardware.

I definitely believe security is a function of quality – or quality is a function of security. You can look at it reasonably both ways.

NSCI: Dr. Boyson, would you briefly describe the cyber supply chain reference model developed by your team?

BOYSON: We made a diagnostic that the state of cyber supply chains currently is about where physical product supply chains were over a decade ago, in terms of fragmentation, lack of a common management structure, etc.

Based on the best practices we had gathered from different cyber experts and on our own knowledge, Hart Rossman, Thomas Corsi and I constructed a cyber supply chain assurance model.

The model started with three nested rings. At the inner core ring is the notion of core governance. By governance, we mean pulling together the right executives who have the power to look across the extended supply chain and act as a systemic risk governance structure for a supply chain.

At the second tier, or the ring around the inner governance ring, is system integration. Those are the people who, on a daily operational basis, manage the construction and ongoing integration of the components of the system. The system integrators can be external – as in the case of "let's go outside and hire a lifecycle contractor" – or it could be an internal function – someone or some group internally that are designated to integrate systems on the company's behalf, such as a company's systems engineering group. That's the second tier and their goal is to keep a handle on the ongoing system risks that are emerging through the various phases of the system life cycle, and keep track of software vulnerabilities, hardware integrity and network robustness. The integrators have the task to keep it all operating in a way that satisfies the stakeholders and the key purchasers of the system. It's a big job, but it can be done.

There are incentive structures that government or companies can provide to move in that direction. They need to incentivize end-to-end coordination across the chain as a way of getting a handle on what has become an increasingly globalized group of actors trying to coordinate together.

The third ring is the actual hardware manufacturers, software developers and the network providers. In each of these realms, they have their own best practices. For example, looking for common weaknesses in software or trying to look at issues of network intrusion detection.

Again, our key diagnostic is that what is missing is a *common* risk governance structure and a common registry of risks that can provide transparency to the overall IT supply chain.

As a result of continued funding and collaboration with SAIC, we have been working on Phase 2 of the model. We have taken our model and tested it with three major organizations. We've held very interesting focus groups, in which we've discussed the model and mapped the model against what presently exists in that organization. We think the model has a lot of explanatory power in terms of charting the key process and communication disconnects that prevent systemic risk management.

NSCI: Mr. Rossman, how should public and private organizations defend against supply chain attacks on their IT systems?

ROSSMAN: The first thing they need to do is begin to have the right conversations, as Dr. Boyson pointed out, between the right risk managers in the organization. When someone suspects something's wrong or suspects that they may have been compromised or that there might be a counterfeit product in their supply chain, there needs to be – already in place – the right mechanisms for incident response, supply chain risk management, IT security, acquisition folks, etc., to be able to deal with that in a holistic manner and to have a common, cooperative incident response capability.

Right now, in most public and private organizations, if you call their computer incident response team and say you believe there's a problem with your software – maybe a virus or a worm, or you think a hacker might be in your system – they know exactly what to do. They have templates, processes and procedures and, organizationally, they know who to reach out to and what the goal is.

If you call that same organization and you suspect you have a hardware problem – maybe a piece of counterfeit hardware or you think there's a value-added component that does something malicious – they won't know what to do. They don't have the templates, they don't have the processes and procedures, and they don't have the organizational relationships to know who else to reach out to to address the problem. We need to build those processes and we need to build that community around incident response. That's the first thing.

The second thing we need to do is be able to manage vulnerability and risk across the supply chain. This idea of having a risk council composed of a number of different elements – as our model shows, the three different levels – to reach across the supply chain and provide risk orchestration and risk registry, so that we're not just dealing with the various risks in a stovepipe manner, but we're dealing with it more holistically and from a position of strength. What's going to drive that is better visibility into the cyber supply chain. What I mean by that is we need intrusion detection systems that span the IT supply chain and are inter-organizational; we need them to look at the network; we need them to look at the software development environment; we need to look at the supply chain and logistics management acquisition systems. We need to bring all of that together and have a common operating picture – a common sense of visibility – across the supply chain to register and orchestrate the management of risks that we're seeing.

I think that we're going to see some public-private partnerships that will necessarily rise as we gain greater visibility in the supply chain. And I think that, although supply chains are global, there are dominant supply chains in a variety of industries. We're going to begin to see some best practices arise in those dominant supply chains that kind of bleed off into the others, so we're going to raise the body of knowledge and raise the consistency of practice across the community, despite having competing supply chains.

NSCI: Dr. Boyson, what part will domestic and international collaboration play in preparation and defense tactics?

BOYSON: That's an interesting question. From what we're hearing, the European Union, in particular, seems to take a more collaborative approach than we do. They seem to be further along in defining a partnership model between the public and private sectors. We think that's really important.

Earlier this year, I participated in a panel at the RSA cybersecurity conference. Represented on the panel were NIST, DoD, the General Services Administration and the National Academy of Sciences. I was representing academia on that panel. What really impressed me was how open the government entities involved in supply chain risk management are and how urgent they felt was the need to partner and collaborate with the private sector. I was also impressed with how the private sector is eager for the government to tell them how they can help. We see a lot of movement right now of major companies and federal agencies trying to figure out the rules of engagement for how to collaborate. We're seeing a lot of out-of-the-box thinking on how to make that happen.

NIST is developing very grounded and interesting Supply Chain Risk Management (SCRM) guidelines and a set of recommendations. People are looking at what NIST is going to come up with on the civilian side of the house. As you know, DoD has its own SCRM policies and procedures.

How important is it for government and industry to collaborate? It's absolutely crucial. Can you draw a line between my network and your network in this period of rapid IT supply chain globalization?

NSCI: Mr. Rossman, you have been quoted as saying "It is a national security imperative in a global economy that we have confidence in the supply chains of integrated systems and the integrity of the people, processes and technology that comprise them." In your opinion, what positive steps is the U.S. government taking to ensure cyber security in our mega-portal logistics environment today?

ROSSMAN: The government has a number of different programs, one of which is the Comprehensive National Cybersecurity Initiative (CNCI), that talks about Initiative 11 – beginning to do risk management in the ICT supply chain. The administration has done a couple of things. They've pulled together some best practices across government and industry. They are implementing some pilot programs – mostly in the government space – to validate those best practices.

What's probably most visible to people in the supply chain (contractors, consultants and folks who work with the government, in general) is that they've begun to insert – in their Request for Proposals – contract language and acquisition language that specifically requires a couple of things. The most prominent thing is that they're asking for bidders on certain government contracts to, as part of their proposal, to submit a supply chain assurance plan. It will typically ask for a description of a cyber supply chain assurance program that the company has and how they intend to flow that down to their vendors and subs as part of delivery of this particular service or solution to the government. They've done that now with a couple of contracts and, from what I understand, it has gotten a fairly good response from the contractor community.

NSCI: Is there anything else you'd like to add?

ROSSMAN: The biggest thing I can say is we have been thrilled to be able to collaborate with the University of Maryland on this. They are a top-notch academic institution and they have been certified as a center of academic excellence in cybersecurity research, in addition to having the Supply Chain Management Center, which has received all sorts of awards and accolades.

We've been really pleased to work with all of the organizations in government and industry that have contributed to our research. What we're finding is that, because of our research, we're able to have the kind of discussions that really advance the state of the art and the state of practice in the areas we discussed earlier – gaining visibility in the supply chain, focusing on relationships in the SDLC (system development lifecycle), developing good acquisition language and contract language.

We're honestly just pleased to be able to contribute to the state of the art and make everybody a little big safer.