Issues in
Technology Innovation

April 2013

Twelve Ways to Build Trust in the ICT Global Supply Chain

Darrell M. West

Darrell M. West is vice president and director of Governance Studies and founding director of the Center for Technology Innovation at Brookings. His studies include technology policy, electronic government, and mass media.

An analysis of computer production found that 18 different countries supplied key parts of laptops (not including the raw materials such as rare minerals that went into those components). This included eight countries (China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, and Taiwan) that supplied parts for the liquid crystal display, 11 places (China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, and the United States) that were involved with memory production, nine nations (Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, and Vietnam) that worked on the processor, one place (Taiwan) that made the motherboard, and eight countries (China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand and the United States) that compiled parts for the hard drive.[1]

As illustrated by the laptop example, the globalization of commerce and trade has created many benefits. Supply costs have been reduced for many products. Computers and other items can be made of parts from a number of different locales. Countries can specialize in particular goods and companies can focus on the things they do best. Raw materials may come from one area, while manufacturing and production lie elsewhere, and sales and marketing take place in still another place. In this as well as other examples, contemporary commerce involves a complex interchange of hundreds or thousands of individuals, organizations, technologies, and processes across a variety of different continents.

But long supply chains and inadequate or nonexistent product evaluation

before deployment, create a situation where widespread vulnerabilities exist in products and networks that can be exploited by others during design, production, delivery, and post-installation servicing. There are industry-wide risks associated with procurement, transportation, and management. Everything from raw materials and natural disasters to market forces, national laws, and political conflict can be problematic. Problems in one area can cascade elsewhere and magnify risks dramatically for the system as a whole.

These difficulties are not unique to any single company or country. A 2012 Symantec Intelligence Report found that 40.9 percent of malware viruses came from the United States, while 24.9 percent arose from the United Kingdom, 9.1 percent came from Australia, and 4.3 percent originated in India.[2] Indeed, malware has become a common feature of global commerce. Insufficient quality control occurs in many places around the world.[3]

According to John Lindquist, chief executive officer of EWA Information and Infrastructure Technologies, "trust should not be based on where the headquarters is located." Markets are global in scope, and supply chain issues intersect with cybersecurity problems and international trade more generally. A survey of U.S. federal chief information officers found that cybersecurity represented their most important area of concern.[4] Indeed, the ubiquity of vulnerabilities calls for universal, comprehensive, and standardized solutions. We need industry-wide solutions that involve product evaluation and reliance on trusted delivery systems. Particularistic solutions aimed at one part of the ecosystem are not going to be successful.

In this paper, I discuss 12 ways to build trust in the ICT global supply chain. With the assistance of a group of leading experts brought together at the Brookings Institution in February, 2013 plus follow-up interviews, I explore the operational threats and technological vulnerabilities that we face, and make recommendations to identify best practices, standards, and third-party assessment for supply chain assurance.

I argue that vulnerabilities in the supply chain and product development, generally, facilitate a myriad of attack and exploitation techniques, such as unauthorized remote access after product deployment for many malicious activities, degradation of ICT networks, and damage to critical infrastructures. I suggest that developing agreed-upon standards, using independent evaluators, setting up systems for certification and accreditation, and having trusted delivery systems will build confidence in the global supply chain as well as the public and private sector networks that sustain them. These and other types of evaluations make information available to purchasers and therefore give them a firmer basis for product selection.

The Unpredictability of Operational Threats

Unpredictability is the hallmark of contemporary commerce threats. It is hard to know in advance when natural disasters, civil unrest, or economic shocks will occur. Recent years have seen a number of such developments take place with serious consequences for the supply chains of many different companies.

In its study of supply chain risk, the World Economic Forum (WEF) identified five major operational disruptors: natural disasters, conflict and political unrest, sudden demand shocks, export/import restrictions, and terrorism.[5] These problems can without warning threaten operations, the availability of needed raw materials, production and delivery schedules, and vital transportation networks. With the current fragmentation of the value chain and extensive reliance on subcontractors, it has become a major challenge to ensure timely and safe delivery of goods and services around the world.

When asked about threats, 93 percent of the 400 business leaders polled by WEF across 10 major industries said they believed that supply chain risks have increased over the last five years.[6] The combination of the Japanese tsunami, the Great Recession, civil unrest in vital regions, and protectionist sentiments in several countries has led most executives to worry about the global supply chain and think about the particular risks that are posed. Nearly everyone involved in business thinks that managing the supply chain and dealing with the myriad of threats needs to be a major priority for their organization.

Dangers arising from the environment, geopolitical disruption, and economic forces complicate operations in virtually every industry. As stated at our workshop by Don Davidson, the Chief of Outreach, Science & Standards, Trusted Mission Systems & Networks of the U.S. Department of Defense Chief Information Office, his department "buys 1.2 million parts for 20 weapons systems." And in many cases, he pointed out, venders "need to ship it in a week." This puts his agency in a very challenging situation.

Increased reliance on off-shoring and out-sourcing and the globalization of supply chains raises points of vulnerability everywhere along the chain. This risk is exacerbated by the fact that there is inadequate quality control to identify and mitigate vulnerabilities before deployment or during product life. Even one weak link along the supply chain can endanger global delivery schedules far down the production or transportation line. Larry Clinton, President and Chief Executive Officer of the Internet Security Alliance, explained that, "you can't compete in world markets today unless you are using long supply chains." Relying on multiple suppliers improves competition, encourages quality, and reduces overall risk.

Increased reliance on off-shoring and out-sourcing, and the globalization of supply chains raises points of vulnerability everywhere along the chain.

Natural Disasters

A number of recent natural disasters have provided stark evidence of the dangers of supply chain disruption. The March, 2011 earthquake and tsunami in Japan demonstrated clearly how weather and environment-related changes can affect production and distribution networks in many industries. The storm hit an area along the Japanese coast where there were a number of manufacturers. The sudden disaster killed 15,000 people, shut down nuclear power plants in Fukushima, and forced the evacuation of 90,000 individuals following radioactive releases from those operations. The resulting shock severely damaged the supply chains of many companies. For example, Japanese automotive production that month dropped 57 percent below the preceding year.[7] And electrical power shutdowns hurt the electronics industry, due to its role as a parts supplier to manufacturers in China, South Korea, Taiwan, and elsewhere.[8]

Similar problems arose that year when massive flooding hit the northern parts of Thailand and eventually affected 61 of the nation's 77 provinces. Rising waters inundated 1,000 production factories and caused widespread shutdowns in operations and distribution networks. Particularly hard-hit were automobile and electronics manufacturers. Most companies reported substantial reductions in their production. The country is the second largest producer of hard drives for computers and analysts reported that manufacturing of those drives dropped as much as 30 percent for the year.[9] In those kinds of widespread disasters, it is difficult to maintain delivery schedules and meet supply chain requirements. Companies such as Western Digital estimated that it would take at least a year to restore production to their pre-flood levels.[10]

Geopolitical Disruptions

Geopolitical problems can arise from civil unrest in key areas, terrorist attacks, corruption, or laws that restrict global trade and commerce. Raw materials often are located in areas experiencing political turmoil or points of contention among outside powers. Whenever unrest arises in Africa, Asia, the Middle East, or Latin America, it becomes virtually impossible to meet production schedules.

Terrorist attacks can upset oil and gas production, tourism, and other vital industries. Intruders this year briefly stopped production at an Algerian natural gas facility when they seized hostages and engaged in a four-day occupation of the gas plant. The attack led to the killing of 37 foreign workers and unsettled trade and commerce throughout North Africa.[11]

Corruption is a serious problem in many parts of the world. It imposes additional costs on businesses transactions and creates bottlenecks in global supply chains.

Businesses never can be sure where or when problems are going to rise or how demands for bribes or special payments will affect delivery schedules. A report by the United Nations Global Compact found that corruption costs about five percent of global Gross Domestic Product, or around $2.6 trillion each year.[12] A study by the British EPPI-Centre found that "a one-unit increase in the perceived corruption index is associated with 0.59 percentage-point decrease in the growth rate of per capita income."[13]

Protectionist sentiments are problematic when they impose high tariffs, barriers to entry, or laws that are unduly restrictive to trade.[14] Anything that limits trade and commerce raise difficulties for the supply chain. This can include tariffs on individual products, domestic content requirements for whole sectors, or rules requiring domestic partners for international commerce. Scott Charney and Eric Werner of Microsoft argue that "indigenous innovation" requirements on domestic content help secure the supply chain, but do so by limiting commerce and impeding trade.[15]

An analysis by the United Kingdom's Department of Business Innovation & Skills found that 10.4 percent of global imports have been hurt by protectionist measures since 2008.[16] And a World Trade Organization investigation reported that there has been an increase in trade restrictions among the G-20 economies. Rising tensions between the United States and China over trade and cybersecurity threaten commerce in many different areas.[17]

Economic Shocks

Economic upheavals have been a major challenge in recent years. The volatility of exchange rates, commodity prices, and macroeconomic forces has been intense. Businesses can plan carefully around existing configurations only to see them disrupted by alterations in economic circumstances. Reliance on the lowest bidder is challenged when economic prices go up unexpectedly.

Exchange rates can be problematic when short-term fluctuations disrupt business models or make it difficult to cover production costs. A survey by Grant Thornton found that "more than four in 10 (42%) manufacturers report that exchange rate shifts were detrimental to their business over the past year."[18] Currency shifts can affect sourcing decisions, plant location, and capital investments.

Commodity price volatility creates havoc when unexpected shifts make it difficult to maintain quality. Recent years have seen a considerable shift in the prices of energy, metals, and agricultural products. A report by the Organization for Economic Cooperation and Development found the cost of rice has risen nine times, wheat five times, and sugar four times since 2004.[19]

The Great Recession hit many businesses around the world hard and led to

renewed focus on cutting supply chain costs. This reliance on low-cost producers raises the risks of suppliers who are not able to meet ambitious delivery schedules or quality production requirements. It threatens quality control measures when firms substitute inferior products or substandard materials.

The Ubiquity of Technology Vulnerabilities

Digital technologies introduce a number of specific problems associated with the ICT supply chain: denial-of-service attacks, spying on confidential material, counterfeiting and malicious substitution, and redirecting system control.[20] "We are a distributed economy and we need an effective way to communicate needs," indicated Davidson. In Canada, Carey Frey, Director of the Strategic Relationships Office, points out that "no regulatory framework exists for hardware/software safety and security" and there are problems associated with the fact that "traditional government policies and processes impose security requirements after products and systems have been developed".[21]

Firms in nearly every nation encounter these vulnerabilities and require mitigation strategies. In the sections below, I describe the nature of these risks and the problems they pose for information and communications technology. The closing section then makes recommendations on how to improve the ICT global supply chain.

Distributed Denial-of-Service (DDoS) Attacks

One risk facing information systems is denial-of-service attacks in which a large number of service requests arrive simultaneously at a website and therefore overwhelms its servers. These kinds of attacks dramatically slow traffic and can effectively render the site inoperative.

Adversaries can do this by tying up bandwidth or processor time, disrupting routing information, or obstructing communications between the user and server. The result is to obstruct the website and keep regular users from obtaining the desired services or information. The consequences for businesses can be quite serious.

Many of the attacks are directed at financial services companies, electronic commerce sites, or software-as-a-service organizations. Attackers use botnet toolkits to control Internet Relay Chat (IRC)-channels. These are the software packages that enable Internet access. Through repetitive attacks, botnets tie up these communications tools and subvert supply chains. Industry reports have found that distributed denial-of-service attacks increased 19.2 percent in 2012 compared to the previous year.[22]

A report by Arbor Networks found that half of businesses reported DDoS attacks on their data centers in the past year.[23] The shift of storage to the cloud has opened up

new areas of vulnerability in the supply chain and created a number of new risks. Public and private sector organizations are putting more and more of their administrative functions in the cloud.[24] Overtime, mission-critical activities related to supply chain are likely to be based in cloud platforms.

These attacks expose companies to great risks and threaten basic business models. "The key problem," said Senate Intelligence Committee Counsel Clete Johnson, "is the market in all its manifestations is not well informed on how to price the costs and benefits of cybersecurity." Executives can't evaluate the impact of this or other attacks on company stock prices or financial earnings.

The rise of mobile technology, cloud computing, and bring-your-own-device (BYOD) creates threats because many companies have shifted their supply chain management to handheld devices (either tablets, smart phones, or cell phones) or cloud-based providers. Much of the mobile equipment lacks basic security protections. Indeed, one-third of American smart phone users reported they used no password to protect their devices.[25] And cloud-based services move vital infrastructure outside of company domains.

Much of the mobile equipment lacks basic security protections. Indeed, one-third of American smart phone users reported they used no password to protect their devices.

Security experts say that many providers have not upgraded their security protocols in line with potential threats. A number of businesses and governments have not adopted best practices and have not implemented basic security hygiene. Officials complain about cyberattacks and data breaches, but don't take the steps required for self-protection. This makes it difficult to safeguard information technology and keep the supply chain open and operational.

Spying on Confidential Information

Spying on confidential material is an age-old problem. In the pre-digital world, it took the form of physical surveillance of other people or organizations. Individuals tracked other people and reported back to their superiors.

In the contemporary world, though, much surveillance comes in electronic form. For example, intruders deploy listening devices or install code that takes over webcams and allows for audio or video spying. They also can break into computer systems and steal proprietary information via spyware. These programs exploit vulnerabilities in operating systems or web browsers, and use security holes to take credit card, financial, or product information that has value to other organizations.

"Ransomware" has become a more common tactic. Intruders use keylogging software, backdoor viruses, and the theft of passwords to gain access to proprietary information and use that information to demand illicit payments from companies in return for not making that material public.[26]

Half of the Forbes 2000 company executives interviewed said they had Risk Committees, but most did not have strong procedures in place to mitigate those challenges.

The U.S. Federal Trade Commission recently charged several American firms that rent computers to consumers with actions that "spied on consumers using computers that consumers rented from them, capturing screenshots of confidential and personal information, logging their computer keystrokes, and in some cases taking webcam pictures of people in their homes."[27] Through these practices, the companies captured financial data, tax identification numbers, private emails, credit card statements, and confidential passwords.

Despite these and other cybersecurity threats, survey evidence shows that many companies "are not undertaking key oversight activities related to cyber risks, such as reviewing budgets, security program assessments, and top-level policies; assigning roles and responsibilities for privacy and security; and receiving regular reports on breaches and IT risks."[28] Half of the Forbes 2000 company executives interviewed said they had Risk Committees, but most did not have strong procedures in place to mitigate those challenges.

Counterfeiting, Trade Secret Theft, and Malicious Substitution

Another threat comes in the form of activity that substitutes one product, service, or software for another or steals trade secrets. This can be as simple as basic counterfeiting. For example, a company can promise to deliver 25 software packages but only 18 are authentic and functioning. Or firms may use false labeling or substitute material of lesser quality for those designed at a higher level.[29] The theft of trade secrets quadrupled between 1988 and 2004 and became a serious problem.[30]

In the ICT area, it is estimated that only 20 percent of microchips are made in the United States.[31] If companies abroad substitute inferior electronic goods, they create performance problems, and health or safety risks. This is true in electronic devices, pharmaceutical products, toys, and consumer items. A United Nations report of counterfeit seizures at European borders found that 57 percent of the products involved clothing, shoes, and accessories, 10 percent jewelry and watches, 7 percent electrical equipment, 6 percent medicine, 4 percent CDs and DVDs, 4 percent toys, and 4 percent cosmetics.[32]

A report by the Organization for Economic Development and Cooperation estimated that 1.95 percent of global trade involved counterfeit or pirated tangible goods.[33] This does not include services or non-tangible products or good sold domestically. Other analyses have put that number at 5 to 7 percent.[34]

Beyond simple counterfeiting, some attackers employ Trojan horse programs that trick people into installing programs that have a malicious purpose. An analysis undertaken by Kaspersky Lab shows how these actions combine spear phishing mail attachments and backdoor .exe files that rely on common software programs to gain entry and substitute pernicious code.[35]

Alternatively, intruders may install keystroke programs that record keyboard entries and transmit them electronically to other people. The result is loss of information and communications systems that don't perform the tasks that consumers and businesses want.

As companies such as package delivery carriers, manufacturers, and suppliers deploy "tap and pay" devices or inventory tracking mechanisms, near-field communications (NFC) equipment enables thieves to engage in "bump and infect" intrusions that use "mobile worms" to infiltrate electronic devices.[36] According to Lindquist, the biggest risk today is "the surreptitious insertion of malware into the system without regard to when in the life cycle it is inserted."

Redirecting System Control

Some malware redirects system control and allows people outside an organization to direct basic computer functions at another time. They use software with command-and-control features to take over particular activities. Their code can make computers do something different than what was intended, and usually do so without the user's knowledge.[37]

Competitors can gain access to system functions through vulnerabilities in web browsers or holes in security systems. Many systems based on HTML5 have figured out how to close risks linked to plug-ins. However, widespread reliance on JavaScript APIs raises web-based vulnerabilities. Users who rely on them risk network intrusions.[38] Yet these and other types of vulnerable software continue to be broadly used.

These types of large-scale attacks are more fundamental than the risks cited above. They may be designed to bring down an entire company or seize control of a specific critical mission. In this situation, the challenge for businesses is how to safeguard their supply chain when crucial functions are compromised.

Twelve Ways to Build Trust

There are a number of initiatives underway to deal with operational and technology vulnerabilities associated with the global supply chain. Some of these efforts focus on businesses because the bulk of critical infrastructure is privately owned, while others work to improve government acquisitions and procurement as a way to disseminate best practices. All of them bring together stakeholders from a variety of areas in an effort to forge an agreement on crucial issues. What is needed are collaborative efforts across countries and companies that recognize the universality of the vulnerabilities and the need for evidence-based mitigation.

In this section, I outline 12 promising ideas to improve trust in the supply chain. I identify management, operational, and technology practices that will improve business functioning and promote assurance. Without those actions, companies around the world will remain at risk from threats that disrupt production, upset delivery schedules, and insert malware into hardware, software, and firmware.

Recommendation 1: Recognize That Most of the Supply Chain is Owned by Businesses and Solutions Require Public-Private Partnerships

Focusing on a few key problem areas and developing public-private partnerships makes more sense than building complicated systems that are difficult to implement and no one truly understands.

In many countries, most of the supply chain is owned and operated by private companies.[39] This puts the primary impetus for securing the supply chain on commercial businesses. Governments should recognize that they have an important role to play, but having too many standards or a proliferation of specifications is self-defeating because it overwhelms suppliers and vendors. Focusing on a few key problem areas and developing public-private partnerships makes more sense than building complicated systems that are difficult to implement and no one truly understands.

This sentiment was articulated by Dan Reddy, Product Manager, Product Security Office of EMC at our workshop. He said "industry is partnering with the public sector to create practical and measureable global standards to address supply chain risk. Industry is pushing back against unique requirements for each geolocation which isn't scalable in today's global interconnected economy." Yet if governments and businesses don't demand stronger protections, it will be hard to assure security for the system as a whole.

An example of a promising public-private effort is the Open Group Trusted Technology Forum, a non-profit group consisting of 400 representatives from business,

government, academia, and non-profit organizations. It seeks to achieve objectives through "open, vendor-neutral IT standards and certifications." Its mission statement lists four objectives: 1) working with customers to capture, understand and address current and emerging requirements, establish policies, and share best practices, 2) working with suppliers, consortia and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies, 3) offering a comprehensive set of services to enhance the operational efficiency of consortia, and 4) developing and operating the industry's premier certification service and encouraging procurement of certified products.[40]

Among its signature initiatives has been the publication of a Provider Standard Snapshot. This is a standard for global companies which produce or buy Commercial Off-the-Shelf (COTS) products. It shows companies how to implement best practices within their organizations and ways to build assurance in IT products. In particular, it focuses on counterfeit products, tainted items, and other types of "non-genuine" assets. Developing verifiable criteria for assessing global supply chains is central to its activities.

In April, 2013, the Open Group published its provider standard on mitigating tainted and counterfeit products. This standard presents "a set of organizational guidelines, requirements, and recommendations for integrators, providers, and component suppliers to enhance the security of the global supply chain." It focuses in particular on Commercial Off the Shelf (COTS) products.[41]

Recommendation 2: Use Labeling and Tracking Chips To Improve Metrics

Technology is part of the problem in supply chains, but it also can become part of the solution. The use of labeling and tracking chips helps at virtually every level of the supply chain. It now is possible to "track and trace" in real time the shipment and delivery of goods from the point of purchase, and thereby judge how well quality is being maintained in various parts of the production cycle.

A report by the U.S. National Institute of Standards and Technology (NIST) says "labeling (e.g., serial number) and tagging (e.g., radio-frequency identification [RFID] tag) software packages and modules, hardware devices, individual elements, and processes that surround them can be used for this purpose."[42]

Companies can monitor performance and request quarterly reports by suppliers for each serial number and find out what happened to each part. Suppliers can keep records on how many parts are scrapped and how they are destroyed. At our workshop, Edna Conway, Chief Security Strategist for Cisco's global supply chain, emphasized that "it's all about the right security technology, physical security practices and logical security processes in the right node of the supply chain at the right time. At the same

time, we need to embrace suppliers as we build security solutions throughout the end-to-end supply chain. Our supply chain partners must be integrated into the design and implementation of any security solutions that we hope to be successful."

Recommendation 3: Deploy Identity Verification Systems

Having single sign-on and personal identity verification systems improves accountability in the supply chain. NIST is developing a "production and operations management" system that integrates planning, production, and scheduling. Using a "virtual, distributed, supply chain integration testbed," researchers have put together a supply chain platform that verifies identity, uses applications software and simulations to monitor compliance, test adherence to stated specifications, and management strategies for securing the supply chain.[43] Controlled access with individual log-ins and outs helps build confidence in the security of the supply chain.

A lack of risk metrics complicates many current mitigation efforts. It is hard to know how serious the problem is in the absence of clear data. Global supply chains involve many countries, a large number of suppliers, and complicated operational logistics. We lack data on many pieces of the supply chain so it is hard to assess risks, mitigation, or compliance. One metric that can be developed at the end of the supply chain is analysis of software for vulnerabilities and for unauthorized code insertion.

In the counterfeiting area, for example, it is difficult to estimate the magnitude of the problem. There are few direct indicators of illegal product substitution and most studies rely on anecdotal evidence, consumer surveys, or law enforcement seizure records. A number of existing studies rely on single countries or particular industries only.[44] Better metrics and identification systems would help companies identify problems and configure possible solutions.

Recommendation 4: Rely Upon Independent Assessments

Many observers think that supply chain problems are unique to particular countries or firms. But EWA chief technology officer Steven Clemmons disputes this notion. He says "there is not much basis to trust any vendor. For example, any major vendor likely has a Chinese footprint in terms of manufacturing or software design and development." Companies from Apple and Cisco to most telecommunications firms rely on facilities based in China. And many Chinese firms buy components from American-based companies.

A 2012 Veracode State of Software Security Report found there are increasing "security risks from third party and externally developed software." Its Vice President

of Research Chris Eng noted that "a typical enterprise has an average of 600 mission-critical applications, about 65% of which are developed externally, leaving companies increasingly vulnerable to the security risks found in these apps."[45] Despite these vulnerabilities, most companies deploy products with little testing or verification, even if they operate within high-risk areas.

...if governments or companies select low verification models when more robust approaches exist, often to save money, they knowingly are exposing themselves to greater risks. They therefore bear considerable culpability for intrusions that occur due to their own short-sightedness.

Regardless of the national origins of the products, what is needed is independent assessment that evaluates underlying software and hardware. Labs need to analyze the source code to identify malware and vulnerabilities that cannot be detected by conventional testing approaches. Hardware and firmware should be assessed to see "what functionality is delivered," and to insure the absence of "hardware backdoors and other exposures," noted Clemmons.

Some approaches provide a complete, independent verification of all deployed software, precluding opportunities for vendors or third parties from deploying undocumented and unevaluated changes. For hardware, these approaches require that a statistically significant random sample of products undergo an independent and comprehensive verification of the boards to insure that undocumented and unevaluated changes have not been made after the initial evaluation. Deployment can then be implemented not by the vendor but by a trusted third-party engineering service provider. These processes are components of what is currently called Trusted Delivery. Trust is enhanced when evaluation results "rise to the level of evidence, and isn't just a smart person's opinion," argued Clemmons.

There is an argument that if governments or companies select low verification models when more robust approaches exist, often to save money, they knowingly are exposing themselves to greater risks. They therefore bear considerable culpability for intrusions that occur due to their own short-sightedness.

Recommendation 5: Develop Integrated Management Tools

Many companies lack assessments tools for monitoring their supply chain or assessing network risk. A study by the University of Maryland Robert H. Smith Business School of 290 IT small business vendors found that "47.6% of the sample never uses a Risk Board or other executive mechanisms to govern enterprise; [and] 46.1% never uses

an integrated IT supply chain dashboard/control."[46]

For this reason, Maryland researchers suggest that firms develop integrated management tools and use benchmarking metrics to track performance. Their TM Forum calls for "making security measurable: Define, contract and implement key performance indicators to prevent threats, end-to-end, in the supply chain".[47]

Some initiatives, according to Jon Boyens, Senior Advisor, Computer Science Division of NIST, are "too stove-piped" and focus on internal operations and upstream suppliers as opposed to governance policy or downstream customers. Additionally, specific hardware and software supply chain practices differ, by necessity, and are dictated by the unique nature of their respective domains. This creates challenges when developing comprehensive ICT supply chain risk management guidance and often results in very high-level standards and practice, making meaningful validation and verification difficult for greater assurance."

Many organizations would benefit from seeing how they compare with other ones. Benchmarking is a good way to get good supply chain practices into product development, as is the comparison of like products at the end of the supply chain. If companies are evaluated on quality performance, they need incentives to do the best possible job. There must be consultation between industry and government to make sure requirements don't become too burdensome.

One notable effort is the Information Security Forum, a non-profit organization made up of leading businesses from the Fortune 500 and Forbes 2000. Its members are "dedicated to investigating, clarifying and resolving key issues in information security and risk management, by developing best practice methodologies, processes and solutions that meet the business needs of our Members." The ISF compiles research, writes briefing papers, and performs benchmarking studies for companies and business sectors. Its "Benchmark as a Service" online tool enables companies to assess their security practices, benchmark results, and compare their performance against other companies around the world.[48]

The Department of Defense (DOD) has taken steps in this direction through the development of a Supply Chain Risk Management Threat Assessment Center. It helps companies evaluate threats and share best practices. According to DoD's Davidson, its Application Specific Integrated Circuits are designed to enhance vulnerability detection and mitigate technical risks in manufacturing, engineering, testing, and evaluation.

The DOD is part of an interagency supply chain group that works to improve supply chain practices and combat counterfeit products. As part of the U.S. National Defense Authorization Act, the department is required to undertake a supply chain study that outlines risks and proposes specific remedies to address those threats. A report on criteria is due by fall 2013 that places responsibility on defense contractors to

assure their products. Among other things, contractors are required to detect and avoid counterfeit products, undertake correction action in case counterfeits are uncovered, and establish procedures to use trusted suppliers for defense products.

The QuEST Forum represents ICT service providers and suppliers around the world "dedicated to improving operational and supply chain quality and performance." Among its top priorities are encouraging the adoption of TL 9000 as a global quality management standard, sharing industry best practices, benchmarking industry performance, and offering new products and services. Its members include service providers from the United States, Europe, Asia, and Latin America.

An American effort is the U.S. Interagency Supply Chain Working Group.[49] It is made up of representatives from the Departments of Homeland Security and Defense, the National Security Agency, and the National Institute of Standards and Technology, among others. It seeks to coordinate federal policies on the global supply chain, although it is focusing more on the physical supply chain than cybersecurity. In particular, this group is interested in supply chain risk management for federal procurement and ways to insure secure products in all aspects of government acquisitions.[50]

Recommendation 6: Improve Information Sharing

One challenge is the difficulty of sharing information in a situation of competitive markets and litigation risk. Companies sometimes are reluctant to share proprietary data out of fear it will expose them to lawsuits or legal liability.[51] They worry that data sharing will put them at a competitive disadvantage or expose them to legal risks from data breaches or counterfeiting.

The Center for Responsible Enterprise and Trade is a non-profit organization that works with "multinational corporations to foster innovation and economic prosperity by protecting intellectual property rights, fighting corruption and driving responsible business practices in global supply chains and business networks." Its mission is to improve supply chain practices through online assessments, training programs, and independent evaluations. It has developed leading practices for intellectual property protection and anti-corruption activities.[52]

In its review of supply chain challenges, the Center proposes that companies "increase information sharing to strengthen supply chain integrity" and "include provisions in supplier contracts that facilitate and improve oversight."[53]

British authorities have launched an innovative international cooperation effort on cybersecurity. Working with the U.S. Department of Homeland Security and National Security Agency, the Australian Defence Signals Directorate, and its own Cyber Security Evaluation Centre, the government agencies share information on threats and remedies.

Each organization has streamlined its procedures in an effort to reduce cybersecurity risks.

The U.S. Government Accountability Office (GAO) has called for outcome-oriented metrics to gauge the effectiveness of efforts to protect communications networks. In its review of Department of Homeland Security cybersecurity activities, the GAO says federal departments and their private sector partners need to "share information on outages and incidents." This will improve cybersecurity and help organizations manage their ICT supply chains.[54]

Recommendation 7: Safeguard Software

Information and communications technology is a particular problem in terms of the supply chain. To help deal with challenges in this area, software companies have designed a SAFECode process that is intended to build "robust assurance practices into each step of the software development process."[55] Companies voluntarily collaborate on assessment standards in order to build confidence that products and services are functioning and non-malicious and perform what they claim to do. This is an example of a best practices approach that is transparent at various stages of the design process.

Another approach is the Open Software Assurance Maturity Model, developed by independent software consultant Pravir Chandra as part of the Open Web Application Security Project and provides tools to measure security, evaluate existing products, and generate software security scorecards. The group provides reviewers and evaluators who help firms implement sound security practices.

The Building Security in Maturity Model uses data from 51 leading software security initiatives to measure safety. It has 134 members drawn from different firms who can obtain security products under a creative commons license. Each year, these people hold an annual private conference and share best practices from across the industry.

Software tagging represents still another way to build security. It is possible to install a software identification (SWID) tag that records the name, version, and usage of each application. This allows companies to track inventories and manage their supply chains. It is a way to use technology to improve security by promoting greater transparency and accountability with digital assets.

Microsoft Windows 8 software has a "secure boot" technology designed to prevent modification of firmware. It seeks to prevent malware from infecting software during the booting up process. This approach addresses an important supply chain risk by giving users greater confidence that their software does not have malicious features that may have been added during production or distribution.

Recommendation 8: Develop Standards to Improve Performance

The development of agreed-upon standards is another area that is very promising.[56] NIST has focused on developing standards at the levels of organization, mission, and operations. Since the federal government is a big purchaser of goods and services, the agency seeks to improve federal acquisitions, according to Boyens. The hope is that securing improvements there will filter out into other parts of the production and delivery systems.

Going forward, NIST and the White House are developing a cybersecurity framework designed to encourage voluntary supply chain standards for suppliers and systems integration for customers and users. Due to opposition from some U.S. industry groups, the federal government is not adopting mandatory requirements of the type favored by the European Union. This means that some firms will adopt the voluntary standards, while others do not. That will perpetuate holes in the security system that will be exploited by hackers and intruders.

Over the next eight months, NIST has been asked to develop integrated management systems and standards for supply chain assurance. It held its initial public workshop on April 3, 2013 in order to get feedback on this framework. These types of tools will help companies manage risks, deal with operational challenges, and mitigate vulnerabilities in their supply chains. Even though the standards will be voluntary in nature, they will guide federal procurement activities. The hope is that their guidelines will promote best practices more generally throughout the commercial sector.

The Alliance for Telecommunications Industry Solutions (ATIS) brings together top global technology companies to address top business priorities. Its cyber security group seeks to "develop the standards and solutions that are creating the future of the information and communications technology (ICT) industry." It represents 166 different companies and works through committees and forums, and is a major contribution to the International Telecommunication Union and the Inter-American Telecommunication Commission. Its top priorities are IP-based infrastructures, converged multimedia services (including IPTV), enhanced operations and business support systems, and improving service quality and performance. It is a member of the American Standards Institute.[57]

SAE International includes over 128,000 engineers and technology experts who write standards focused on the aerospace, automotive, and aviation industries. They emphasize the hardwa re side of production and are designed to encourage sound production practices.

The International Organization for Standardization develops standards using technical committees of experts from commercial providers. It has produced 19,500

The major thing to be careful with in establishing formal standards is that they evolve with the underlying threats. Sometimes, according to Clemmons, the standards development and acceptance process "takes too long while the real world threat evolves too quickly."

standards over the past several decades in areas such as quality management and risk management. Participants from different countries have developed standards regarding change control, logical access control, and physical access control. This includes mechanisms to determine who enters and exits facilities, times of entry and exit, verifying access, controlling entry, securing keys, detecting physical tampering, and maintaining safeguards such as guards, alarms, and monitors.[58] This gives companies a uniform way to improve supply chain security and build trust in global trade.

The United Kingdom works on security standards through its Cyber Security Evaluation Centre and its National Technical Authority for Information Assurance. Through this agency, this agency serves central government departments, the British Health Service, and its Critical National Infrastructure. It produces standards focused on inventory control, tagging, management controls, access controls, registration and verification requirements, and digital signatures, among other things. Companies that wish to get certified submit their products for approval through the Centre site.

The Centre takes an active role in managing public sector security. It focuses on standards as a way to assure product quality and makes sure that major government departments follow these standards. It also imposes strict rules on the use of memory devices thought to create real or potential vulnerabilities. For example, to protect its information systems, the United Kingdom requires memory sticks to be encrypted when used by government officials.[59]

The major thing to be careful with in establishing formal standards is that they evolve with the underlying threats. Sometimes, according to Clemmons, the standards development and acceptance process "takes too long while the real world threat evolves too quickly." We need standards that are sufficiently flexible that they enable maintaining currency against developing threats and other challenges.

Recommendation 9: Certify Promising Procedures and Processes

Certification presents a way for companies to gain confidence in the supply chain. By having uniform procedures for safeguarding quality, it is possible to build greater confidence in the system as a whole.

An example of this is the Common Criteria for Information Technology Security

Evaluation certification program. Group members have established standards and procedures for IT quality control that must be met in order to be certified for security evaluations.[60] Among the items reviewed are "personnel identity, access controls to product assets, secure development processes, integrity controls over development and distribution, and anti-counterfeit measures."[61] Countries such as the United States, United Kingdom, Australia, New Zealand, Turkey, Japan, France, Canada, South Korea, Germany, Italy, Malaysia, Netherlands, Norway, Spain, and Sweden have signed on to these protocols. However, some observers such as the U.S. House Permanent Select Committee on Intelligence have criticized this effort as inadequate and claimed it has not produced the desired results.

The U.S. Federal Risk and Authorization Program is another example in the government procurement process. Companies can get particular products certified for government use across all federal agencies. It is a way to evaluate software solutions and open up their usage across the federal government. Previously, each agency certified its products individually and there was no guarantee that a product certified by one department would qualify for another.

The British Cyber Security Evaluation Centre has announced a certificate program for IT professionals. It is designed to raise "the level of cyber security competence in the UK".[62] Those who enroll get training at three levels of certification: practitioner, senior practitioners, and lead practitioner, and the program covers areas such as security officers, auditors, risk advisors, and architects, among others.

Canada requires that "the Contractor must not deploy any equipment on Canada's network or on its own or 3rd party network infrastructure or backbone that will be interconnected with Canada's network unless that equipment has been externally evaluated by a recognized certification body approved by Canada."[63] It also has mandated that government data be stored on equipment located within the country.

For some, though, standards are more important than third-party assessment. "[I]t is cheaper to evaluate yourself," said Davidson. In his view, organizations should audit their producers against agreed-upon standards.

Recommendation 10: Accredit Strong Performers

A number of people have proposed accreditation as a way to build assurance control. This allows third-party assessors to certify that companies meeting certain standards are publicly acknowledged as being accredited for good performance. Accreditation can be based on meeting agreed-upon standards, but it is important to describe the scope and nature of the accreditation. As suggested by Conway, "the key is to clearly define representative processes, products, and practices which render a

supply chain security certification meaningful to the potential technology acquirer."

The Open Group Trusted Technology Forum is developing a standard and related trusted accreditation process to aid efforts to secure the global supply chain. Having established a set of best practices, it allows companies to submit information demonstrating whether they have met those operational standards. The accreditation is good for three years, and companies can apply for re-accreditation.

Reddy pointed out that accreditation is organizationally-based, not product-based. Reviewers examine organizational processes and quality management to see if they pass reasonable thresholds for quality assurance. This makes it different from certification of particular products.

It is important to keep certification and accreditation up-to-date. Lindquist noted that "most certification and accreditations are snapshot views of what conditions were at the time of the certification audit." The half-life of particular technologies may be six months to a year rendering the audit out of date.

Recommendation 11: Conduct Audits to Identify Special Problems

Post-performance audits allow outside organizations to come in with spot inspections or reviews of performance and quality assurance. Conway asserts that "a small set of international standards is a path to enhanced security industry-wide." She noted that "while OEMs use audits, spot inspections and security integrated into supplier performance metrics, certification or accreditation to such standards requires recognized auditors and international certification laboratories."

Some companies use product evaluation as a form of audit. They conduct regular audits of products as a way to assure their quality and reliability. They review a sample of items shipped to determine whether they perform as advertised and meet agreed upon standards. "Given the threat landscape, industry-wide standards and best practices should be developed and implemented to ensure that products are evaluated – from post-production to delivery to installation to post-installation servicing and updates – to safeguard against the introduction of vulnerabilities or malicious capabilities," said Andy Purdy, chief security officer at Huawei Technologies USA.

Many auditors today are focused on particular products, but it is important to build up the supply of qualified reviewers. "No one has all the expertise today," noted Johnson. "We need a community of experts." The lack of identified, suitable experts complicates efforts to build benchmarking and auditing into the supply chain.

Recommendation 12: Distinguish Low, Moderate, and High Risk Problems and Devise Remedies Appropriate for Those Threat Levels

Traditional risk management notes that not all threats represent the same degree of vulnerabilities. Some are higher risk and call for stronger remedies than others. For example, NIST distinguishes low, moderate, and high risk areas and suggests increasing levels of mitigation as products move from low to high risk.

From its standpoint, businesses need to investigate several aspects of supplier organizations and build relevant assurance. This includes features such as company history, the robustness of production processes, foreign influences, exploitable vulnerabilities, supply chain weaknesses, and overall track record.[64] To improve the supply chain, the agency calls for a "multipronged, mission-driven" approach of risk assessment based on tougher federal acquisitions regulations, the adoption of international standards, improved data sharing, and using technology and online tools to track supply chain practices.[65]

Conclusion

To summarize, I argue that problems in the ICT global supply chain are not limited to any locale, but are common features of global commerce. Long supply chains, weak product evaluation, and the voluntaristic nature of many proposed remedies weaken our ability to address common threats. We need more sustained, integrated, and comprehensive approaches to operational and technological threats. We have to improve use of standards and third-party assessment in order to provide supply chain assurance.

There clearly are problems and vulnerabilities in many spots along the global supply chain. As companies and government agencies increasingly rely on commercial off-the-shelf products, it is very challenging to make sure that software, hardware, and operations meet secure standards. Firms must share information on which products are reliable and secure to build the sense of trust that is so vital to the overall system. There must be greater certainty about the relative assurance and security of competing products and whether malicious software or hardware was added along the supply chain or the products otherwise contain exploitable vulnerabilities.

Nearly a dozen large U.S. business associations have argued that singling out particular countries for punitive actions is counter-productive. Many American technology firms rely on components made or assembled in China. Saying that government agencies should not rely on Chinese products ignores the risks that exist at every point along the supply chain. The U.S. Chamber of Commerce, the Semiconductor Industry Association,

the Telecommunications Industry Association, Tech America, and BSA/The Software Alliance rightfully note that "product security is a function of how a product is made, used, and maintained, not by whom or where it is made."[66]

Following recent U.S. passage of legislation that placed limits on the ability of federal agencies to purchase products from Chinese technology companies, the Obama administration complained that the restriction "could prove highly disruptive without significantly enhancing the affected agencies' cybersecurity."[67]

We need to figure out ways to build trusted networks and evaluate how current efforts meet important objectives. The ideas presented in this report outline a number of operational and technology initiatives that mitigate risks through best practices, independent evaluation, agreed-upon standards, certification, accreditation, and auditing of supply chain practices.

In each of these activities, the goal is to develop trusted networks and third-party validators that improve the quality of supply chain operations and the assurance level of products and networks. Trusted delivery systems with reasonable transparency, accountability, and reciprocity are needed so that vendors feel confident about distant partners. Without that kind of trust, it is hard to maintain quality in long supply chains around the world in the areas of consumer goods, pharmaceuticals, defense, food, automobiles, or technology.[68]

But whatever standard, certification, or accreditation that is developed must have a dynamic component. Sandy Merber, Counsel, International Trade Regulation and Sourcing at General Electric, says "we want to make sure the certification process doesn't become part of the problem. It is a very dynamic area. Systems must be refreshed over time."

Endnotes

Note: I wish to thank Elizabeth Valentini for her valuable research assistance on this paper.

1. Gregory Wilshusen, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks." Government Accountability Office, March, 2012, p. 5.
2. Symantec, "Intelligence Report," December, 2012, p. 7.
3. Georgia Institute of Technology, "Emerging Cyber Threats Report," 2013, pp. 4-5 and Georgia Institute of Technology, "Consensus Cyber Security Controls," March 6, 2013.
4. Tech America, CIO Survey, 2012, p. 4.
5. World Economic Forum, "New Models for Addressing Supply Chain and Transport Risk," 2012, p.4.
6. World Economic Forum, "New Models for Addressing Supply Chain and Transport Risk," 2012, p. 7.
7. Fujita Masahisa and Hamaguchi Nouaki, "Japan and Economic Integration in East Asia: Post-Disaster Scenario," RIETI Discussion Paper Series 11-E-079, December, 2011.
8. Hidetaka Yoneyama, "The Lessons of the Great Tohoku Earthquake and Its Effects on Japan's Economy," *Fujitsu Research Institute*, April 8, 2011.
9. Simeon Ang, "Thailand Floods Disrupt Supply Chains & Raise Inflationary Risks," Shares Investment, November 4, 2011 and Thomas Fuller, "Thailand Flooding Cripples Hard-Drive Suppliers," *New York Times*, November 6, 2011.
10. Fang Zhang, "Thai Floods Continue to Impact Hard Drive Manufacturing," Applied Market Intelligence, February 12, 2012.
11. Adam Nossiter, "Chad Says It Killed Algeria Hostage Crisis Mastermind," *New York Times*, March 3, 2013, p. 4.
12. United Nations Global Compact, "Fighting Corruption in the Supply Chain," June, 2010.
13. Mehmet Ugur and Nandini Dasgupta, "Evidence on the Economic Growth Impacts of Corruption in Low-Income Countries and Beyond," London: EPPI-Centre, Social Science Research Unit, Institute of Education, University of London, 2011, p. 2.
14. United Kingdom Department for Business Innovation & Skills, "Protectionism: Trade and Investment Analytical Papers," 2011.
15. Scott Charney and Eric Werner, "Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust," Microsoft Corporation paper, July 26, 2011, pp. 6-8.
16. United Kingdom Department for Business Innovation & Skills, "Protectionism: Trade and Investment Analytical Papers," 2011, p. 4.
17. World Trade Organization, "Report on G-20 Trade Measures," May 31, 2012.
18. Grant Thornton, "Supply Chain Solutions," *World Trade Magazine*, 2010.
19. Organization for Economic Cooperation and Development, "Competition and Commodity Price Volatility," 2012, p. 23.
20. Edna Conway comments at Brookings Institution Supply Chain Workshop, February 4, 2013.
21. Carey Frey, "Cyber and Supply Threats to the GC," Communications Security Establishment Canada, June 12, 2012, p. 29.
22. Prolexic, "Quarterly Global DDoS Attack Report," Q4, 2012, p. 2.
23. Arbor Networks, "Worldwide Infrastructure Security Report," 2012, Volume VIII, p. 7.
24. Paul Wormeli, "Mitigating Risks in the Application of Cloud Computing in Law Enforcement," IBM Center for the Business of Government, 2012.
25. *Time*, "How Has Wireless Technology Changed How You Live Your Life?," August 27, 2012, pp. 34-39. This Time Mobility Poll was undertaken in cooperation with Qualcomm between June 29 and July 28, 2012.
26. McAfee, "2013 Threats Predictions," 2013, p. 5.
27. Federal Trade Commission, "FTC Halts Computer Spying," September 25, 2012.
28. Jody Westby, "Governance of Enterprise Security," CyLab Report, 2012, p. 5.
29. CREATe, "Health and Safety Risks From Counterfeits in the Supply Chain," October, 2012, p. 8.
30. CREATe, "Trade Secret Theft: Managing the Growing Threat in Supply Chains," 2011, p. 6.
31. Jason Miller, "Agencies, Vendors Ramping Up To Fight Supply Chain Cyber Threats," *DoD News*, June 15, 2012.

32. United Nations Office on Drugs and Crime, "The Globalization of Crime," undated, p. 178.
33. OECD, "Magnitude of Counterfeiting and Piracy of Tangible Products," November, 2009, p. 1.
34. United Nations Office on Drugs and Crime, "The Globalization of Crime," undated, p. 173.
35. Kaspersky Lab, "'Red October' Diplomatic Cyber Attacks Investigation," 2013.
36. McAfee, "2013 Threats Predictions," 2013, p. 4.
37. Scott Charney and Eric Werner, "Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain," Microsoft Corporation paper, 2012.
38. McAfee, "2013 Threats Predictions," 2013, p. 10.
39. Telecommunications Industry Association, "Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain," 2012, p. 2.
40. Drawn from the About Us section of the Open Group website at http://www3.opengroup.org/aboutus.
41. The Open Group, "Open Trusted Technology Provider Standard Version 1.0." April, 2013.
42. Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles, "Notional Supply Chain Risk Management Practices for Federal Information Systems," National Institute of Standards and Technology, NISTIR 7622, October, 2012, p. 28.
43. Shigeki Umeda and Albert Jones, "Virtual Supply Chain Management: A Re-Engineering Approach Using Discrete Event Simulation," undated, p. 8.
44. Stijn Hoorens, Priscillia Hunt, Alessandro Malchiodi, Rosalie Liccardo Pacula, Srikanth Kadiyala, Lila Rabinovich, and Barrie Irving, "Measuring IPR Infringements in the Internal Market," Rand Europe, 2012.
45. Veracode, "Enterprise Testing the Software Supply Chain," November 12, 2012.
46. University of Maryland Robert H. Smith Business School, "Assessing SCRM Capabilities and Perspectives of the IT Vendor Community," 2012, p. 88.
47. TM Forum, "Securing the Cyber Supply Chain," Morristown, New Jersey, 2013, p. 19.
48. Taken from its website at http://www.securityforum.org.
49. White House, "National Strategy for Global Supply Chain Security," January, 2012.
50. National Institute of Standards and Technology, "Supply Chain Risk Management for Information and Communications Technology," January 7, 2013.
51. Jarrellann Filsinger, Barbara Fast, Daniel Wolf, James Payne, and Mary Anderson, "Supply Chain Risk Management Awareness," Armed Forces Communication and Electronics Association Cyber Committee, February, 2012, p. 6.
52. Material drawn from its website at www.create.org.
53. CREATe, "Health and Safety Risks From Counterfeits in the Supply Chain," October, 2012, pp. 17-19.
54. Government Accountability Office, "Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts," April, 2013, p. 31.
55. Software Assurance Forum for Excellence in Code, "Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain," June 14, 2010.
56. John Suffolk, "Cyber Security Perspectives," Huawei paper, 2012, p. 19.
57. Summarized from its website at www.atis.org.
58. Tyson Storch, "Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity," Microsoft Corporation paper, July 26, 2011, pp. 7-9.
59. Chris Mayers, "Information Assurance as a Flexible Security Solution," Info Security, January 19, 2012.
60. Common Criteria, "Common Criteria for Information Technology Security Evaluation," September, 2012, Version 3.1, Revision 4.
61. Scott Charney and Eric Werner, "Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust," Microsoft Corporation paper, July 26, 2011, p. 12.
62. The Chartered Institute for IT, "BCS Certify Information Assurance Professionals for Government Departments Including CESG," October 9, 2012.
63. Communications Security Establishment Canada, "Technology Supply Chain Guidelines," October, 2010, p. 11.
64. Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles, "Notional Supply Chain Risk Management Practices for Federal Information Systems," National Institute of Standards and Technology, NISTIR 7622, October, 2012, p. 20.
65. Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles, "Notional Supply Chain Risk Management Practices for Federal Information Systems," National Institute of Standards and Technology, NISTIR 7622, October, 2012, p. 1.

66. Brendan Sasso, "US Industry Rallies Against Ban on Chinese Tech Products," Hillicon Valley, April 4, 2013 and April 4, 2013 letter signed by 11 major U.S. industry groups.
67. Brendan Sasso, "White House Criticizes Ban on Technology Products From China," *The Hill*, April 5, 2013.
68. Scott Charney and Eric Werner, "Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust," Microsoft Corporation paper, July 26, 2011, pp. 8-9.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor
Beth Stone
Donna Ra'anan-Lerner

Production & Layout
Beth Stone

Email your comments to gscomments@brookings.edu