Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust

Scott Charney, Eric T. Werner[1]

July 26, 2011

[1] This paper benefited from the many reviewers who provided substantive comments and helped to shape this paper. An alphabetical list of contributors can be found in Appendix A.

Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Authors

Scott Charney – *Microsoft Trustworthy Computing*
Eric Werner – *Microsoft Trustworthy Computing*

Preface

Governments worldwide have begun to express concerns about the threat to their Information and Communications Technology (ICT) systems from the global supply chain for ICT products. These concerns are based on the risk that an adversary might tamper with products during their development, manufacture, production or delivery. In response to these concerns, some governments have begun to develop policies and requirements intended to mitigate these supply chain risks.

This paper introduces Microsoft's perspective on supply chain risk and the relationship of such risk to global trade in ICT products. It reviews the considerations that lead governments to express concerns about supply chain security and discusses the implications of some approaches to "solving the problem." It points out the importance of having national approaches to supply chain risk management that are risk-based, transparent, flexible and reciprocal or standards-based.

A companion paper, titled *Toward a Trusted Supply Chain: A Risk Based Approach To Managing Software Integrity,* details Microsoft's approach to assessing the risks to its supply chain and enumerates the classes and locations of controls that Microsoft has employed to manage that risk.

A World of Growing Cyber Dependencies Fuels Supply Chain Concerns

It is now incontrovertible that the Internet has transformed the way we live and work, and that it has presented both immense opportunities and challenges. We also now accept without debate that (1) Information and Communications Technology (ICT) systems are indispensible to critical infrastructures and government operations; (2) society faces a host of threats to these ICT systems, including cybercrime, economic espionage, military espionage, and cyberwarfare; and (3) there are many attack vectors used to attack these systems, including exploiting vulnerabilities, exploiting configuration errors, exploiting older or unpatched systems, and social engineering.

Over the course of the last decade, critical infrastructure protection (CIP) initiatives have taken root in many countries.[2] But in light of our dependency on cyberspace, increased concern about cyber threats, and increased appreciation of the globalization of the development, manufacture, and maintenance of ICT systems, there is one other attack vector receiving increased attention: concern that sophisticated adversaries will taint the supply chain, inserting functionality into products and services that grants one entity control over another organization's ICT systems, perhaps to steal information, alter information, or deny service at a critical moment.

[2] The 2009 International CIIP Handbook surveyed and documented efforts in as many as twenty-five countries and seven international organizations. International CIIP Handbook 2008/2009, Center for Security Studies, Eidgenösische Technische Hochschule Zürich (A. Wenger, V. Mauer, M. D. Cavelty, ed.).

The Nature of Cyber Supply Chain Risk

Supply chain risk can take many forms, with some scenarios more plausible than others. Thus, it is useful to begin with a clear delineation of the nature of the problem. At a basic level, the concern is that an adversary may sabotage, maliciously introduce unwanted functions, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system in order to conduct surveillance or to deny access to, disrupt, or otherwise degrade its reliability or trustworthiness.[3] Addressing these sophisticated and malicious threats is the principal concern that animates much of the government activity surrounding cyber supply chain security today, and it is this concern that this paper attempts to address.

Government concerns about supply chain risk to their critical communications and information systems are understandable. In a world of diverse and competing economic, political, and military interests, no country wants to be dependent on products and services that may be tainted by an adversary. Government perception of growing supply chain risk can be traced to the globalization of the international ICT market and a growing appreciation of the cyber risk environment.

Not very long ago, in the days of "plain, old telephone service" (referred to as "POTS"), the international market for telecommunications equipment was dominated by a small handful of vendors from an even smaller number of countries, and many telephone companies were, in fact, government run (or government influenced) services. Three decades of telecommunications privatization, ICT innovation, and free-trade policies have led to a broad diversity of ICT products being made by a broad array of vendors, with products being deployed and serviced globally. This advance of technology and change in ICT business models has increased the opportunities for sophisticated, hostile actors to leverage these systems to achieve malicious consequences on a scale that would not have been possible in the past. While these conditions may create uncertainties and apprehensions, this open trade environment has also contributed significantly to lowering ICT costs, increasing competition, creating jobs, catalyzing economic development, increasing social interactions, and contributing to the technical innovation that has fueled the explosive growth of the Internet and online services.

[3] See, for example, the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, H.R. 6523, 111th Cong. § 806(e)(4) (2011) (definition of "Supply Chain Risk"). It is also worth noting that there are other types of "supply chain" risks that are unrelated to adversarial conduct. For example, the tragic earthquake and tsunami in Japan illustrate a classic type of supply chain risk: automobile manufacturing at plants around the world was halted due to a shortage of critical parts. But while such natural disasters are often addressed by business continuity plans, protecting one's supply chain from deliberate adversarial conduct represents a very different problem, one that implicates national security and public safety in a very different way.

For both governments and the vendors that support them, the challenge of managing supply chain risk is also compounded by complexities inherent in the supply chains themselves. The supply chains that support the delivery of information and communications products and services consist of globally-distributed and dynamic collections of people, processes and technologies that encompass numerous hardware and software components. The risks, therefore, are not subject to easy quantification and remediation; it is difficult to know whether a process, hardware component, or a complex piece of software has been subject to malicious manipulation or modification because available testing capabilities cannot provide satisfactory answers to that question.

How Governments Have Responded

Harboring apprehensions about their dependence on foreign entities for critical national needs, and confronted with the complexities of the vendor supply chain risk environment they do not control and lack adequate tools to assess, national governments have taken different approaches to supply chain risk. While all of these responses are rooted in security-based concerns and often adopt risk management principles, the approaches may have different levels of impact on both trade and innovation due to how such principles are operationalized.

United States

By way of example, Initiative 11 of the Comprehensive National Cybersecurity Initiative (2008) provided the overarching policy framework for the United States, stating that:

> *[r]isks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and re-sources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global market-place; and partnership with industry to develop and adopt supply chain and risk management standards and best practices* [4]

Following from these principles, the U.S. National Institute of Standards and Technology (NIST) developed a draft set of practices to address life cycle supply chain risk for high-impact Federal information systems across acquisition, development, and operation.[5] NIST's draft Interagency Report (IR) 7622 (Draft NISTIR 7622) is rooted in the notion that critical information systems and their components "are at increasing risk of supply chain attacks from adversaries enabled by growing technological sophistication and facilitated by the rapid globalization of our information system infrastructure, suppliers, and adversaries."[6]

[4] *See* http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[5] Piloting Supply Chain Risk Management Practices for Federal Information Systems, (DRAFT) NIST IR 7622, June 2010.

[6] *Id.* at 1. The paper further observes that "[a]ccelerating trends in multinational mergers and acquisitions of information system suppliers and integrators is making it almost impossible to adopt corporate ownership and control alone as the basis for assuring supply chain security." *Id.*

Consistent with these principles, Section 806 of the National Defense Authorization Act for Fiscal Year 2011 authorizes the Secretary of Defense or the Secretaries of the Army, Navy, and Air Force to exclude vendors or their products if they pose an unacceptable supply chain risk.[7] Similar proposals to modify Federal Acquisition Regulations more broadly to address supply chain risk in the context of government procurement actions are also included in omnibus cybersecurity legislation now pending in Congress.

India

India's policy documents contain language reflecting similar supply chain concerns. For example, its discussion draft on its National Cyber Security Policy states that:

> *[i]ncreasingly, nations are also concerned that the ICT supply chain could be influenced or subverted in ways that would affect normal, secure, and reliable use of information technology. Inclusion of malicious hidden functions in information technology can undermine confidence in products and services, erode trust in commerce, and affect national security.*[8]

While the supply chain concern may be stated similarly, India's response has been markedly different. Instead of focusing on the exclusion of vendors and products that pose unacceptable risks, the Indian government attempts to reduce that risk by relying upon policies promoting "indigenous innovation".

China

China, like India, looked to indigenous innovation to help manage supply chain risk.[9] As a part of its 11th five-year plan, China launched an aggressive indigenous innovation effort, which placed a high priority on investing in domestic research and development, including in all segments of the ICT sector from chips to hardware and software. Consistent with this view, China initially required an indigenous innovation product catalog be used for its government procurement and adopted its Administrative Measures for the Multi-level Protection of Information Security (Multi-Level Protection Scheme or "MLPS").[10]

[7] Ike Skelton National Defense Authorization Act for Fiscal Year 2011, H.R. 6523, 111th Cong. § 806 (2011).

[8] Discussion Draft on National Cyber Security Policy, Ministry of Communications and Information Technology, Government of India (April 2011) at 5.

[9] Notice of the Ministry of Finance on Distributing the Administrative Measures on Government Procurement Contracts of Products with Independent Innovation, Ministry of Finance, Government of the People's Republic of China, April 3, 2007: the government's procurement of goods from outside China "shall be constantly regulated in such a way as to establish a system for evaluating foreign products and methods to manage imported products. In addition, an effective means to encourage the purchase of indigenous innovation products shall be established." Moreover, the Notice further prescribed that "those entities that have been approved for the purchase of foreign products . . . should uphold the principle that is in favor of understanding and utilizing core technologies; and give priority to award contracts to those foreign companies transferring core technologies." *Id.*, Article 11.

[10] Article 21, Multi-Level Protection Scheme Management policy document No. 43, issued June 22, 2007.

The MLPS imposes several requirements on security products destined for use in Level 3 or above information systems,[11] including the following:

1. The entity that researches, develops and manufactures the product must be invested or controlled by Chinese citizens, legal persons or the state, and have independent legal representation in China;

2. The core technology and key components of products must have independent Chinese or indigenous intellectual property rights;

3. The entity that develops and produces the product must confirm that the product contains no functions or programs that are intentionally designed as a vulnerability, backdoor, or Trojan;

4. Products that have been listed in the Certification and Accreditation Administration of People's Republic of China (CNCA) catalogs of information security products must acquire a certificate issued by the China Information Security Certification Center (ISCCC); and

5. For products containing encryption technology, the MLPS requires approval from the Office of State Commercial Cryptographic Administration (OSCCA), and no imported products with encryption functionality can be used without approval.

Russia

Finally, Russia has long implemented a certification regime that focuses on non-disclosed functionality (NDF). The NDF certification regime specifically seeks to address concerns about backdoors and other "functions" that might not be disclosed to users. In a move that has some parallels to those undertaken by India and China, Russia is also creating a "National Software Platform" to help reduce dependence on foreign products and, arguably, to support domestic innovation.[12]

[11] The MPLS defines Level 3 systems as "the compromised information systems [that] cause serious damages to social order and public interests or harm to national security."

[12] See, "Russia to adopt Linux as national operating system by 2015," http://www.geek.com/articles/news/russia-to-adopt-linux-as-national-operating-system-by-2015-20101228/ ("Russia's move to divorce its IT infrastructure from relying upon an American company's operating system seems like another small step away from relying upon America"). On the impact on innovation, see "The list of software that must be created in Russia," http://www.sprintspeedstories.com/the-list-of-software-that-must-be-created-in-russia/ ("Among the goals are listed import substitution, national security, the elimination of the backlog in the level of IT usage in the economy and the competitiveness of domestic developments in the global market").

Indigenous Innovation

As discussed in the previous section, an approach to addressing supply chain concerns that has found popularity with some national governments has focused on policies encouraging "indigenous innovation"; that is, policies that seek to promote domestic development, sourcing, and manufacture of information and communications technology, equipment, and services. This approach is reflected in the Indian government's consultation document on its domestic telecommunications sourcing policy which observes that "[l]ocal manufacture can also help in addressing security and safety concerns."[13]

The impact of such an approach may, of course, extend beyond security. For example, while noting the contribution that indigenous innovation policies can make to security, the consultation document also makes clear that there are competitive economic benefits to promoting indigenous innovation:

> The telecommunications industry is enabled by a complex value chain that includes equipment suppliers, service providers, and users. The telecommunications value chain begins with sourcing of components like semiconductor chips and software. These components are, in turn, incorporated into equipment purchased by service providers. The service providers then use the equipment to build networks and provider [sic] service to the end users. The equipment manufacturers also supply terminal equipment like mobile and fixed telephone instruments to the end users. India has been able to drive innovation when it comes to software services in the telecom space. But the results are not so encouraging when it comes to developing telecom equipment. To become an important player in the global telecom space, India has to create a synergetic telecom ecosystem and build globally competitive product companies across the telecom value chain.[14]

China, like India, looked to indigenous innovation to help manage supply chain risk.[15] As a part of its 11th five-year plan, China launched an aggressive indigenous innovation effort, which placed a high priority on investing in domestic research and development, including in all segments of the ICT sector from chips to hardware and software. Consistent with this view, China initially required an indigenous innovation product catalog be used for its government procurement and adopted its

[13] Consultation Paper on Encouraging Telecom Equipment Manufacturing in India, Telecom Regulatory Authority of India (TRAI), Dec. 28, 2010, at 3 ¶ 3.

[14] *Id.* at 1-2 ¶ 2 (emphasis added). To further underscore the point, the TRAI goes on to state that "[t]he larger issues in front of us are to see how the telecom manufacturing value chain needs to be altered to benefit the Indian telecom industry and the country and what needs to be done to make India a telecom manufacturing powerhouse." *Id.* at 3-4 ¶ 4.

[15] Notice of the Ministry of Finance on Distributing the Administrative Measures on Government Procurement Contracts of Products with Independent Innovation, Ministry of Finance, Government of the People's Republic of China, April 3, 2007: the government's procurement of goods from outside China "shall be constantly regulated in such a way as to establish a system for evaluating foreign products and methods to manage imported products. In addition, an effective means to encourage the purchase of indigenous innovation products shall be established." Moreover, the Notice further prescribed that "those entities that have been approved for the purchase of foreign products … should uphold the principle that is in favor of understanding and utilizing core technologies; and give priority to award contracts to those foreign companies transferring core technologies." *Id.*, Article 11.

Administrative Measures for the Multi-level Protection of Information Security (Multi-Level Protection Scheme or "MLPS").[16]

While such stringent rules in favor of indigenous innovation may help manage supply chain risk, they clearly serve as a major impediment to those seeking to import products into the China market. Additionally, such rules may harm China's exports because if China's approach were adopted by other countries, those countries would also require the use of locally created products, thus restricting the use of Chinese products in other countries. Perhaps recognizing that fact, the China Ministry of Finance announced, on July 1, 2011, that it had eliminated its indigenous innovation product catalogs and de-coupled indigenous innovation products from government procurement preferences, thus balancing its desire to promote domestic innovation and reduce its dependency on foreign products and services with its interest in promoting global trade and economic development.

[16] Article 21, Multi-Level Protection Scheme Management policy document No. 43, issued June 22, 2007.

Elements of the Trust Problem

Whatever their purpose, national policies codifying preferences for domestic suppliers create trade barriers, undermine foreign investment, and deprive domestic industry of the benefits of technological innovations from elsewhere in the world. The question becomes, therefore, "how do countries protect national security interests without inappropriately undermining the value produced by a global supply chain?" The answer to that question requires understanding the elements of the trust problem and formulating a meaningful and workable framework for addressing supply chain risks. Fundamentally, supply chain concerns fall into four categories: (1) products from distrusted countries; (2) products from distrusted companies; (3) distrusted or tainted products; and (4) insufficient or unknown processes related to supply chain integrity.[17]

(1) *The product comes from a distrusted country.* Countries may have competing or adversarial interests that generate a significant level of mutual caution or distrust. In such cases, one country may be hesitant to rely upon products and services coming from the other and, in the most extreme cases, may seek to ban all products and services from a second country inviting, of course, a reciprocal response. Such an approach will, if applied beyond the most sensitive national security applications, fragment the global market, seriously impact free trade, and undermine the economic and innovation advantages that come from a global marketplace. Equally important, if there is a "presumption of distrust," vendors may be barred from important markets regardless of how rigorous or well-designed their supply chain risk mitigation practices may be.

(2) *The product comes from a distrusted company.* Although this concern may often be rooted in the fact that the company is located or headquartered in a distrusted country or is perceived to have a particularly close relationship with its own government (that is, it is really a matter of "distrusted country"), a buyer's concern could stem from other considerations (e.g., the company may be a front for an organized crime syndicate).

(3) *The product itself is distrusted or tainted.* Circumstances may also arise where a government possesses specific, concrete information that a particular product or service has been compromised.[18] In these instances, the case for exclusion of a vendor or product – from a government procurement action or from the market as a whole – is most compelling. But even then, a government's decision to exclude a vendor or product is not without issues. For example, if the basis for the government's concern rests on sensitive or classified information (*e.g.*, from a law enforcement investigation or intelligence source), a government may be unwilling or unable to disclose the information fully to either the vendor (who may be unaware of the issue and, if it knew, would take corrective action) or customers (who may be

[17] It is worth noting that "countries" and "companies" are legal constructs; in the end, people make and operate products and services and it is ultimately people who will undermine supply chain integrity. But those people may be distrusted because they are agents of (or simply sympathetic citizens of) a foreign state, agents of an organized crime group, or merely disgruntled employees in an environment where the risks they pose are not well managed. Thus, it is appropriate to focus on the underlying cause of concern, even if people are the ultimate actors.

[18] The fact that a product is tainted does not necessarily mean the vendor itself is involved in any misconduct. For example, an employee of the vendor may be responsible for the taint and, as a result, the vendor's primary interests may be in eliminating the taint and discharging the employee.

dependent on the product too). Even if the government were willing to share the information, such sharing would clearly undermine the vendor's position in the marketplace, something that is particularly problematic if the information turns out to be false.

(4) *The product comes from a company that is neither distrusted nor located in a distrusted country, but the adequacy of the company's supply chain risk mitigation processes is questionable or inadequate.* This final category involves situations where there is no presumptive reason to distrust the provider, but there are concerns about whether the provider has taken reasonable steps to manage supply chain risk. This last point requires further elaboration. Practically speaking, the supply chain risks of greatest concern are those that originate from, and are executed by, nation state military or intelligence organizations for the purpose of conducting espionage or, perhaps, gaining tactical advantage at a key moment. Notwithstanding the seriousness of the issue, it must be expected that (1) vendors of COTS products will manage supply chain risk in commercially reasonable ways; and (2) governments must manage any residual risks through their own internal practices. Put another way, supply chain risks cannot be eliminated entirely by vendors or, for that matter, by enhanced government procurement processes. Nor can they be completely eliminated by governments by using domestic products created and managed by local people. In sum, governments must have appropriate expectations regarding what supply chain risks vendors can mitigate and recognize that achieving further risk reduction may require governments to adjust their own internal business processes to safeguard against any residual risks. That said, vendors can and should be expected to take steps to manage supply chain risk. There is much that can be done, especially if governments, industry, and users adopt the right set of over-arching principles.

The Path Forward: Principles and Practices to Help Governments Manage Risk in the Supply Chain

It has often been noted that protecting cyberspace requires a public-private partnership, in large part because the private sector is responsible for designing, deploying, and maintaining most of the world's critical infrastructures. To the extent that supply chain concerns also pose risks to that infrastructure, it follows that the public-private partnership should focus on this issue too. More specifically, there needs to be broad agreement on the principles that govern supply chain risk management, followed by concerted public and private action to adhere to those principles. In that regard, supply chain efforts must be (1) risk-based, utilizing collaboratively developed standards; (2) transparent; (3) flexible; and (4) reciprocal. Additionally, the public-private partnership should create an agreed-upon framework for managing supply chain risk at a tactical level. A common framework has many advantages: it would give vendors some degree of certainty concerning the security standards that they would be expected to meet and audited against, the nature of the assurances required to demonstrate compliance, and confidence that assessments were being conducted in a uniform and even-handed manner. It would also provide a baseline against which vendors could measure their own practices against their peers, thereby helping all companies improve their risk management performance.

1. Risk-based approach

The complexities of today's ICT supply chains – which increase the difficulty of evaluating supply chain integrity -- make it tempting to employ a simplistic approach, one that relies on presumptions of untrustworthiness based upon national origin or some other readily identifiable factor. There are several reasons, however, why such a simplistic approach is flawed both in principle and in practice. First, vendors have a significant economic incentive to resist the efforts of national governments to taint the supply chain for a very simple reason: there is a significant risk that back doors or other intentional defects will be discovered and made public, and such a revelation will lead to loss of public trust, and, ultimately, market share. Indeed, it is likely that a company engaging deliberately in such activities may be forced out of business, especially if one appreciates that the loss of trust would be global; that is, even people in the vendor's home country are likely to reject a product with secret backdoors, even if they were inserted primarily so that the local government could obtain advantage against foreign adversaries. In many countries, there is concern not just about foreign surveillance, but domestic surveillance as well.

Second, a simplistically imposed ban cannot eliminate risk from the most concerning of adversaries; there will always be residual risks that must be managed. Simply put, there is no way to prove that even a domestically created and maintained product has not been tainted, either during development or after deployment. Thus, even if it is true that residual risk is reduced by relying upon purely domestic product, a risk management process is still required.

Third, some of the most important products and services upon which the world relies, such as servers, routers, and personal computers, are actually composite products that are globally sourced. For example, a computer may have chips designed in one country, manufactured in a second country, and then loaded with software from yet other countries. Since many complex products cannot be tied to a single country, all countries using those products share some degree of risk.[19] From a practical perspective, the global character of many products also means that attempts to ban products based upon country of origin will result in many products being banned broadly, a result which requires the abandonment of open trade principles and giving up the benefits of global innovation.

Since supply chain risk must be managed regardless of where a product is designed, created, or maintained, it is important to start with fundamental risk management methodology. Classic risk management principles require identifying key assets, enumerating the threats to those assets, implementing and testing controls to mitigate those threats, and establishing an incident response procedure to be used in the event of an incident. While in some cases it may be clear that a certain asset is a key one (that is, it is important to national security and public safety), there may be other cases where only the user of the product fully understands the asset's true value, perhaps because of unique knowledge about where that asset is deployed and the functions it supports. The problem is compounded because commercial off-the-shelf software products are designed to meet a broad range of functions and, in many cases, are relied upon in scenarios involving high value assets that could not be addressed in advance by the vendor. This being true, it may be difficult to know when higher levels of assurance are necessary absent good communication between governments and the vendor community.

Next, it is important to develop robust threat models to help identify and prioritize supply chain risks. Today, companies often rely on threat models they have developed themselves and, as such, these threat models may reflect only the vendor's understanding of the risks. In fact, such threat models would be better informed if the vendor understood aspects of the environment in which the product is to be used and the capabilities and intent of those who may seek to exploit the supply chain. In this regard, it is important to integrate private and public sector information to develop more holistic threat models, even if one recognizes that the sensitivity of such information may, at times, make the sharing of information more challenging.

By way of example, some experts believe that tainting an entire product line (e.g., the design of a computer chip or the source code for a widely deployed commercial product) is not an effective way of attacking an adversary because (1) it is difficult for a lone individual or group of people to move a specific set of design flaws through the entire product lifecycle (including conception, design, engineering, manufacturing, shipment, and delivery); (2) such a broadly deployed taint is more likely to be discovered; and (3) such an attack is less likely to be successful because there is no guarantee that the tainted product will be where it needs to be, when it needs to be there. That being true, it may be more likely that an individual product will be tainted shortly before it is delivered to its intended recipient. In other cases, especially with ICT systems that need continual maintenance, the risk might relate to remote access through maintenance ports or the

[19] It could be argued that the playing field is not really level simply because countries are dependent on the same products, especially if some countries are willing to exploit their portion of the supply chain and others are not. That said, few countries are likely to take comfort in the fact that their adversaries may be too principled to seek an advantage.

delivery of updates after delivery, an activity that does not require the product to be tainted from its inception.[20] The critical point is that supply chain risk must be considered throughout the product's entire lifecycle (from design to maintenance to retirement) and each risk (including personnel, physical and IT risks) must be enumerated clearly.

Even if a vendor would not deliberately taint its own products, specific risks must still be identified and mitigated effectively. Again, it is important to appreciate the threat model and what mitigations can reasonably be employed to manage those risks. For example, a product user may be concerned that a foreign adversary has planted an employee in the vendor's company with the goal of tainting a product without the employer's knowledge. While effective personnel identity management, combined with access controls and other measures to protect against product tampering, can reduce the opportunities for malicious exploitation of supply chain vulnerabilities, it is unlikely that a person inserted into the development process for nefarious purposes would have personal history that makes his or her intentions obvious (or, put another way, it is unlikely that a background check on the employee would readily reveal that (s)he is the agent of a foreign power).

Still, if we return to the concept that this is about risk mitigation – not risk elimination – then adopting sound business practices throughout the supply chain process can serve to reduce the opportunity for compromise or subversion of a product during the product's lifecycle and, thereby, reduce the residual risk that must be managed by the end user. For software companies, processes like those described by SAFECode,[21] which build robust assurance practices into each step of the software development process, can contribute significantly to reducing supply chain risk. Such best practices provide a strong foundation on which to build, but ultimately, governments and members of the private sector should work towards a standards-based framework that all nations can accept as a basis for assessing and making trust judgments about vendors' supply chain risk mitigation practices. Some international organizations have also focused on supply chain risk, such as the International Standards Organization.[22] Other certification regimes, such as Common Criteria (CC), could be extended to cover supply chain risks. If this were done, however, it would be important to ensure that Common Criteria relied upon relevant evidence to evaluate products and processes and that the scope of international participation be increased. Regardless of specific standards that define supply chain best practices, it seems clear that those practices should cover personnel identity, access controls to product assets; secure development processes; integrity controls over development and distribution; and anti-counterfeit measures. Vendors and governments should leverage work in these bodies to develop relevant standards specifically tailored to address ICT supply chain risks. Additionally, it will be important to verify compliance with best practices. There are, at a minimum, three models for verifying compliance, and each has benefits and costs. These include (1) self-certification, which tends to be less expensive but may raise concerns regarding the rigor of the process; (2) independent third party audits, which ensure outside review but can be expensive and time-consuming; and (3) government oversight, which can raise issues of scale due to the sheer number of products that must be reviewed. Of course, one could use different verification regimes depending on the degree of risk; for example, one might permit self-certification for less critical systems and

[20] Of course, operational controls could restrict such access, thus reducing that particular risk.

[21] *See, e.g., Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain*, Software Assurance Forum for Excellence in Code (SAFECode), June 14, 2010; *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain*, SAFECode, July 21, 2009.

[22] *See, e.g.*, ISO 28000 Series, Supply Chain Security Management Systems.

require third party or government audits for more critical systems. Ultimately, however, such processes should be standards-based to provide greater uniformity and certainty for both governments and vendors.

Regardless of the approach taken, it remains important to ensure the right things are being evaluated in the right ways; otherwise, precious resources may be expended to implement practices that do not reduce risk effectively and efficiently. Indeed, in the current environment, the sheer number and diversity of ICT products raises significant challenges and would make the review and assessment of individual products both costly and burdensome for companies and government regulators alike.

Finally, governments and industry should expand basic research, with specific attention given to identifying and developing better metrics for assurance and integrity (that is, better metrics for measuring risk). Additional research may help users assemble trusted systems from untrusted parts (e.g., trusted boot and virtual compartments may shield the customer from some forms of compromise), and it may be possible to identify specific policies, standards, and procedures that allow systems to recover gracefully from supply chain incidents.

2. Transparency

In addition to being risk-based, frameworks to mitigate supply chain risk must promote transparency by all parties. For those who produce and operate products and services, it must be expected that governments will not be content with vendor self-certifications about integrity; rather, they will prefer – as suggested above -- to “trust but verify.” Thus, vendors will need to provide an appropriate degree of transparency into their business processes, and visibility into the controls they use to ensure their product and service development and operations are secure. Indeed, such transparency may prove important not just when a vendor’s practices are questionable or inadequate, but in other cases as well. It was noted earlier, for example, that a vendor may be distrusted solely because it is located in a distrusted country. This “presumption of distrust” can be rebutted by being transparent; that is, by showing that despite its location, its products are not influenced by its local government.

One example of such transparency is Microsoft’s own Government Security Program (GSP), a program that helps address the unique security requirements of national governments by providing eligible, participating governments online access to Microsoft source code for the most current versions and service packs of Windows

Client, Windows Server, Windows CE, and Office.[23] By affording governments an engineering-level perspective of product architectural design and implementation, the program provides enhanced visibility and insight into the integrity of the platform. Moreover, participants in the GSP have the opportunity to visit Microsoft development facilities and discuss our development, testing, and deployment processes with Microsoft security experts.

At the same time that vendors need to appreciate government supply chain concerns, governments need to appreciate that vendors have responsibilities too, such as the responsibility to protect trade secrets and other intellectual property rights, as well as to respect national laws (e.g., export/import control laws). These responsibilities may limit the degree of transparency that is possible. For example Microsoft's GSP allows government reviewers only limited rights (e.g., they may read and reference the source code but may not modify it or make derivative works). Finally, and consistent with Microsoft's responsibility to protect its intellectual property, the GSP is only available in geographic markets that have intellectual property regimes that meet international standards (over 65 such markets eligible to participate in the GSP program). This careful blend of transparency and partnership, coupled with regular interaction, collaboration, and information sharing between Microsoft and governments, has contributed significantly to building mutual trust between the participating governments and Microsoft.

While the GSP may be one example of increased transparency, it is worth noting that such programs are not without challenges. First, governments may lack the expertise to understand the information vendors provide; this is one of the reasons Microsoft provides, along with source code access, the ability to consult with Microsoft security experts. Second, governments may not have sufficient workforce capacity to evaluate the universe of products upon which they rely; a government system or critical infrastructure provider may rely upon products and services from Microsoft, Cisco, Oracle, Symantec and a wide range of other large and small vendors. Again, a return to risk-based principles is important here, as not every product presents the same level of risk within an organization.

Governments, too, have responsibilities if they expect to partner with vendors to find efficient and effective means of managing supply chain risk. For example, if vendors are to be forthcoming with sensitive business information, they should expect that governments will protect that information appropriately and be transparent about how they use such information to assess supply chain risks. Additionally, if a government does have a concern about certain supply chain controls and is not distrustful of the vendor, it should alert the vendor to those concerns and provide the vendor with an opportunity to either correct any inaccuracies or cure any defects. Otherwise, the risk assessment process is secretive and potential adverse actions are not subject to any meaningful and fair review.

3. Flexibility

Frameworks for addressing supply chain risk must be flexible. With various types of suppliers providing ICT systems to governments, there needs to be flexibility in the controls and mitigations that

[23] See *Microsoft Shared Source Initiative, Government Security Program*, additional information available at http://www.microsoft.com/resources/sharedsource/gsp.mspx. The program also affords access to cryptographic code and development tools, subject to requirements such as U.S. government export control approval. *Id.*

a supplier implements based on the technology they are providing. For example, the controls that a hardware supplier needs to implement may have similarities to, but not be identical to, the controls a software supplier needs to implement. Additionally, since governments may face unique threats, vendors may have different business models and market challenges, and threat models may need to be altered quickly in response to changes in technology, having rigid and static supply chain rules in place is not desirable. This does not mean, of course, that national efforts to address supply chain risks must be entirely ad hoc; harmonization and the adoption of international standards to provide a foundation for national approaches is desirable to provide clarity and certainty for vendors around the world. For example, vendors may be expected to have a range of controls (e.g., identity management, access controls, and auditing) in place with regard to the development, manufacture, or implementation of any product or service that poses a significant risk to the customer's security. Similarly, there may be best practices for how to handle the complexities of the supply chain: when vendors rely upon suppliers, there may be contractual best practices and technical controls that help ensure that a vendor's best practices are embraced by its suppliers.

Finally, we should seek to evolve current approaches to internationally accepted standards-based ways of certifying products, such as Common Criteria. The point is that to the extent that the global marketplace does not provide a consistent set of policies, standards and procedures for ensuring the integrity of the supply chain, government and industry should work together to develop a consistent set of best practices, ensure such best practices are codified in international standards, and develop methods to verify that such best practices have been adhered to.

As part of this process, there will be ways to ensure that technology provides the flexibility to meet unique national interests. For example, providing tools that permit customers to manage technology locally can decrease dependence on foreign vendors for post-deployment management. Similarly, by leveraging standards that support cryptologic agility in software development, governments can retain the flexibility to recommend or even require the use of domestic cryptography even when deploying globally available products.

Finally, frameworks for supply chain integrity need to recognize that ICT products and services exist within a highly dynamic environment. As the recent emergence of mobile devices and cloud computing illustrates, both products and services change rapidly, perhaps mitigating some risks and introducing or compounding others. While this certainly adds to the challenge of assuring supply chain integrity, it also highlights the need for flexible risk management approaches. In short, government requirements need to adapt quickly to changes in the risk environment and accommodate differences among vendors, but remain focused on what risks can be mitigated through commercial development and what residual risks remain for governments to address.

4. Reciprocity

Just as trade relationships are based upon the idea that opening markets in reciprocal ways can create trading opportunities between participating countries, it must be recognized that closing markets based upon supply chain concerns will lead to similar "reciprocal" behaviors, potentially balkanizing the Internet and denying people everywhere the benefit of the highly innovative low-cost products that only a global supply chain can produce. The development of international standards for supply chain security will not be simple, but such development is essential if citizens, governments, and suppliers are to continue to realize the benefits of the global Internet while being able to rely on the security and integrity of their ICT systems.

As noted earlier, standardized approaches to supply chain security and risk management are being considered by the International Standards Organization. Additional work is occurring in the Open Group's Trusted Technology Forum, and there have been some preliminary discussions about whether to integrate supply chain security considerations into the international Common Criteria. None of these efforts has yet produced a final product and all have demonstrated that developing standardized approaches to supply chain security and risk management – and the associated certification or evaluation schemes – will be difficult. Nonetheless, if such standards are developed and serve to reduce government concerns about the security of the supply chain, there will be less incentive to enact trade barriers in the name of national security. This fact makes the quest for internationally standardized approaches well worth pursuing.

Of course, trading agreements and national actions restricting such trade, are within the provenance of governments, even if influenced by concerns other than security (e.g., achieving economic advantage). The point is that the amazing global transformation of the last few decades is the product of global free trade and ICT innovation. This suggests that governments need to think very carefully about how to manage the risks presented by a global supply chain, adopting approaches that do not undermine the benefits only a global supply chain can produce.

Conclusion

Across the globe, governments and their citizens are relying on the ICT infrastructure to support commercial, social, cultural, and governmental activities that contribute to the economic security, prosperity, and well-being of their countries. Growing awareness of these dependencies has stimulated increased apprehension about the potential for deliberate manipulation or subversion of these critical national systems through supply chain attacks. While government concerns are understandable, it is important that government responses do not threaten the vitality of the global ICT sector, stifling both innovation and competition.

The diversity of suppliers and the complexity of many ICT products make managing cyber supply chain risk particularly challenging but not insurmountable. Governments need to reexamine their understanding of cyber supply chain risk, recognize it as a shared problem that all countries must now confront, and seek solutions that build bridges rather than exclusionary trade walls. Vendors too must be rigorous in assessing their own supply chain risks and adopting best practices for mitigating those risks across their enterprises and products. By working together, government and the private sector vendor can find common ground for increasing trust in the global ICT supply chain.

Appendix A

During the creation of this paper, many people were provided with drafts or heard briefings and provided extremely helpful comments. In some cases, some individuals provided cumulative comments from their teams and we do not have a complete list of reviewers. In other cases, the concepts in this paper may have been presented at an organized event, and then informed by helpful hallway comments or other conversations after the event. We apologize, in advance, if we failed to recognize any contributor. That said, we do specifically want to thank the following contributors (in alphabetical order): Jing De Jong-Chen, Cristin Goodwin, Ralph Hood, Min Hyun, Steve Lipner, Jenner Mandel, Angela McKay, Paul Nicholas, Sally Nguyen, Glenn Pittaway, P Phil Reitinger, John Stewart, and Tyson Storch.

Microsoft®

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security