Stuffing the Genie Back in the Bottle: Can Threats to the IT Supply Chain Be Mitigated?

by Emilio Iasiello

Introduction

The global information technology (IT) supply chain has been on the forefront of cyber security concerns for several years. First initiated by the Bush administration's 2008 Comprehensive National Cybersecurity Initative (CNCI), the U.S. government identified the need to develop a multi-pronged approach for global supply chain risk management, a theme that has since been underscored by the White House's January 2012 *National Strategy for Global Supply Chain Security*. Both documents agree that the globalization of the IT marketplace has created opportunities for hostile actors to compromise the confidentiality, integrity, and availability of IT products and services. The global IT marketplace is composed of multiple businesses, vendors, and relationships that span countries, regions, and time zones. Federal government agencies must rely on these vendors and commercial-off-the-shelf products to satisfy their IT requirements, which have politicians and security experts clamoring for supply chain oversight. As evidenced by the recent House of Representative report on the Chinese telecommunications companies Huawei and ZTE, the U.S. government fears the possibilities of IT supply chain exploitation by foreign IT companies although it cannot attribute acts of espionage or intentional compromise. This raises two important questions: 1) Is the supply chain threat blown out of proportion as the U.S. government continues to purchase commercial products; and 2) If not, is it too late to mitigate the threats to fragmented global enterprise? Ultimately, securing the global supply chain is as difficult as trying to secure the global Internet and for many of the same reasons. More attention should be spent on ensuring the quality of products being integrated into networks rather than trying to find out if an adversary is going to use this cumbersome global supply chain monolith as a viable means to commit espionage.

White House Releases a Strategy

In January 2012, the White House's *National Strategy for Global Supply Chain Security* bolstered assertions made in the 2008 Comprehensive National Cybersecurity Initiative and those made later in a March 2012 General Accountability Office report that the U.S. is vulnerable to exploitation in the global IT supply chain primarily because the global supply chain is large, unmonitored, and vulnerable to hostile acts at any point of a product or device's life cycle.

What's interesting about the Strategy is that it calls for an integrated domestic effort, as well as an international approach, toward addressing supply chain weaknesses and vulnerabilities as the best way forward to solving this problem. This is disconcerting because it does not offer an alternative to the status quo but tries to operate within its constraints. The Strategy does not encourage

domestic development of indigenously produced IT goods and services as a viable means to counter the supply chain threat, suggesting that the U.S. has no intention of returning to a time when it was a leading developer and manufacturer of IT products. If the U.S. government doesn't cultivate this type of IT production renaissance, then it is doomed to be dependent on what the global marketplace offers. Other countries such as China,[1] India,[2] Iran,[3] and Russia[4] are in the process of trying to develop indigenous computer software and hardware to reduce their dependence on foreign manufactured equipment, and in turn, increase their cyber security posture in the process. The fact that China, Iran, and Russia specifically are suspected of conducting hostile cyber activities against U.S. and foreign targets should serve as a wake-up call to the U.S. government. After all, suspicions of U.S. involvement in the Stuxnet, Duqu, and Flame attacks against Iran were catalysts for Iran to increase its cyber defense apparatus.[5] If our suspected cyber adversaries are seeking to reduce their vulnerability by building in-house, why wouldn't the United States do likewise? However, this is not even a consideration for the United States, which at one time was a technological leader and innovator for computer hardware production, suggesting that profits and global commerce have replaced simple security considerations.

What Is the Supply Chain Threat?

Because of its size and the amount of potential companies involved (depending on the product/service), the global IT supply chain offers numerous potential access points for exploitation at any stage of the development, manufacturing, assembly, and distribution process. Moreover, these threats can appear at each phase of the system development life cycle to include initiation, development, dissemination, implementation, maintenance of an information system. As a result, the compromise of an agency's IT supply chain can degrade the confidentiality, integrity, and availability of its critical and sensitive networks, IT-enabled equipment, and data.[6] According to a 2010 report from Carnegie Mellon's Software Engineering Institute, the identity of a product or a provider may not be discernible to the organization acquiring the product,[7] nor does it have visibility into a supplier's subcontractors. Equipment, parts, or devices to be included into the overall product may be obtained from outsourced companies in other countries, not to mention vendors selling commercial-off-the-shelf products who may outsource their own production.

According to the Government Accountability Office (GAO), an independent, nonpartisan agency that investigates how the federal government spends taxpayer dollars, reliance on a global supply chain introduces multiples risks to federal information systems and underscores the importance of threat assessments and risk mitigation.[8] In a March 2012 report,[9] the GAO identified five major threats to the IT supply chain:

- Installation of hardware or software containing malicious logic
- Installation of counterfeit hardware or software
- Failure or disruption in the production or distribution of critical products
- Reliance on malicious or unqualified service provider for the performance of technical services
- Installation of hardware or software that contains unintentional vulnerabilities

The picture that the GAO paints is bleak; the U.S. government lacks the necessary policies, procedures, standards, and monitoring capabilities to take on this threat, despite having steadily enacted acts empowering agencies for this very purpose. So what we are left to conclude is that any current policies are ineffective; agencies are ignoring their mandates; or no one knows what exactly the next steps that should be taken. In short, federal agencies and related departments will continue to rely on inadequate measures to address the supply chain threat, which begs the question – is it too late to mitigate these threats?

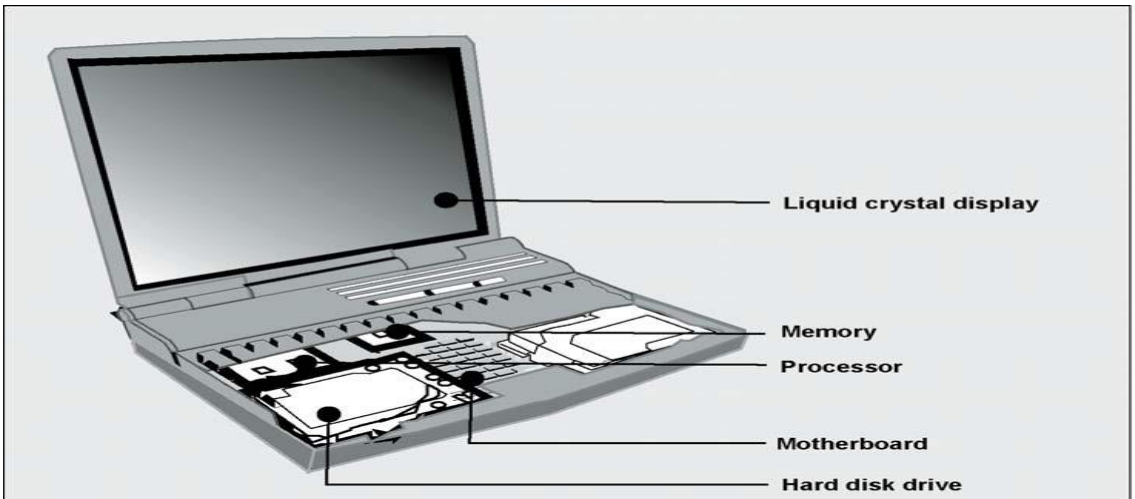
Can Supply Chain Threat be Mitigated?

The supply chain threat is difficult to detect, monitor, and mitigate. A report from the Georgia Tech Information Security Center and Georgia Tech Research Institute characterized such threats as "…expensive to fix, and a policy nightmare."[10] Whether it's the purposeful insertion of malware, the presence of vulnerabilities, or other flawed hardware/software, the IT supply chain presents ample opportunity for intentional or unintentional malfeasance. Below highlights some of the challenges of supply chain mitigation:

- *The Supply Chain Encompasses the World.* The United States surrendered its leadership position in the development and manufacturing of IT equipment in favor of increased profits raised through globalization. Presently, it is rare that a company does all of the manufacturing and assembly of IT goods in one location. An IT product lifecycle that encompasses research and development to product implementation and service, and includes packaging, shipping, and delivery, may occur in several locations throughout the world. Figure 1 taken from General Accountability Office March 2012 report GAO-12-361 illustrates the possible combinations of countries involved in the manufacturing of components assembled into one laptop computer.[11] The number of countries potentially involved in this process represents opportunities for hostile actors to introduce malware into a computer. Even if you purchase a computer from a U.S. or European computer company, the components in the computer will have been made somewhere else.
- *Outsourcing.* An IT customer often does not know if the trusted vendor company he has purchased a product from has outsourced or sub-outsourced any of the production to other companies, and therefore, has no insight into what quality assurance or security standards are used. Asia has been a prime location for outsourcing of global computer components since many of the leading computer manufacturers established research and development centers in China. According to a 2008 report published by the Alfred P. Sloan Foundation, philanthropic, a nonprofit grantmaking institution, "by 2005 China was the single largest producer of personal computers and computer equipment overall in the world."[12]

- *Testing, Testing, Testing.* Conducting an independent analysis of the product will help the identification of an untrustworthy piece of equipment but it is not a foolproof method. For a large government agency making a substantial purchase of computer equipment, the volume of products would take too long to audit individually and be cost prohibitive. Devices such as

host-based security systems can be used to monitor for uncharacteristic behavior and ensure that the systems are working as they should. However, this would increase an organization's cost, requiring additional personnel and technical resources to accomplish this task, which is not guaranteed to catch suspicious behavior.



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information.

Figure 1. The potential countries of origin of the common suppliers for various components within a commercially available computer.

China – A Supply Chain Threat Case Study

China has been identified by the U.S. government as well as other foreign governments as an aggressive cyber espionage actor. According to an October 2011 report from the Office of the National Counterintelligence Executive, cyber espionage activity suspected of originating from China has targeted entities in the following sectors: diplomacy, aerospace, aviation, internet companies, information technology, and the military, to name a few. Linked to global perception of the China cyber monolith is that Chinese information and communication technology (ICT) companies – specifically Huawei and ZTE – support the Chinese government and use their accesses to create backdoors, steal data, or do whatever is asked of them by the government escalating fear and increasing paranoia. The question is simple: do these companies pose a legitimate threat?

The House of Representatives Investigative Report

The Committee highlighted twelve national security threats posed by Huawei and five by ZTE. However, the majority of issues raised by the Committee addressed business practices, decisions, and operations. No compelling case was made for a "supply chain" threat; nor were there any global incidents or events presented to support the Committee's contentions. Although a classified annex was attached to the report that allegedly bolstered the Committee's claims, there was still no evidence linking Huawei or ZTE to espionage activities. It appears that the Committee began their investigation with a presumption of guilt, persecuting Huawei and ZTE on the grounds of what "could happen" rather than what did happen or was happening. Below highlights the Committee's concerns:

1. *China has the means to use telecommunications companies for malicious purposes.*

The Committee made this judgment based on cyber espionage conducted by suspected Chinese actors, as well as the possibility that Chinese intelligence services exploiting the supply chain and use the accesses provided by Huawei and ZTE to insert malware into hardware/software components. The report fails to cite any specific examples of these companies supporting either cyber espionage activity, or implants found in equipment provided by either ICT vendor. Furthermore, the argument is hypothetical; any government can use their telecommunications companies for malicious purposes. Without an example to support this contention, this argument falls short.

2. *Huawei and ZTE failed to satisfactorily explain their relationships with the Chinese government and State Owned Enterprises.*

The Committee based its judgments on the understanding that Chinese government often provides financial backing to industries and companies of strategic importance. Huawei responded that the only connection to the Chinese government was that which is required by Chinese law, and denied any business relationship with Chinese national security organizations such as the Ministry of National Defense, the Ministry of State Security, and the Central military Commission. The Committee's objections on this point were that more information was not provided by Huawei officials. ZTE revealed that it's a publicly traded company on the Shenzhen stock exchange. Its largest stockholder at 30% Zhongxinxin is owned in part by two state owned enterprises – an aerospace company and a microelectronics firm, but that the majority of the company – 70% – was held by dispersed public shareholders. The Committee never indicated the amount of information that would have satisfied their request, only that it wasn't satisfied.

3. *Huawei and ZTE admit that the Chinese Communist Party maintains a Party Committee within their companies but failed to explain what that Committee does.*

Huawei was forthright with offering that the Chinese Communist Party (CCP) maintains a committee in the company, which is required by Chinese law, but that it had no relationship with Huawei's business activities. In ZTE's case, the company acknowledged this as well and provided a

sworn affidavit from its independent director that refuted the government, military, or the CCP's undue influence in ZTE operations. Again, the Committee did not like this answer, preferring to intimate that relationships existed outside the business sphere and that CCP committees provided a shadow source of power and influence without providing any evidence of such activity.

4. Huawei's corporate history suggests ties to the Chinese military.

The Committee pointed out that the founder of Huawei was – but is no longer – a director for the People's Liberation Army (PLA) Information Engineering Academy, and associated with the Third Department of the PLA. This is a weak argument as many former military, intelligence, and government officials leave their former positions to assume leadership positions in the private sector, especially in the United States.

5. Huawei and ZTE refused to provide details on their R&D programs

The Committee requested information on the technologies, equipment, or capabilities that the funding or grants by the Chinese was supporting. Huawei responded that it only bid on research and development (R&D) open to the rest of the industry, and that while it provided telecommunications products for the Chinese military, it did not provide special services to the Chinese military or Chinese security services. The Committee refuted this claim with a copy of an email from a former Huawei employee that related to Huawei provided special network services to an elite cyber warfare unit in the PLA. This claim was never substantiated and the credibility of this source was never offered up for debate. With ZTE the company acknowledged 30% ownership by Zhongxingxin , but did not offer enough details into products produced by Zhongxingxin's subsidiary – an aerospace research institute. In this case, the Committee did not like the fact that it was not given access to the products produced by this institute so that it could evaluate those technologies for military or intelligence applications. This was an unfair request given that the research institute was not the company called into question, nor was it producing telecommunications equipment.

Was this a Fair Report?

From a national security standpoint, the report was not fair as the Committee could not offer any proof or examples of espionage or even suspected espionage activity with Huawei or ZTE. The majority of their concerns focused on potential business practices and quality of equipment intimates that national security concerns were used as a smokescreen to perhaps protect U.S. economic interests. The U.S. has several companies with U.S. government ties (such as Boeing, Motorola, and Oshkosh Corporation) operating in China without fear from the Chinese government or exclusion from the Chinese marketplace.

Further supporting the imbalanced nature of the House report is seen in the October 2012 White House announcement that it had carried out its own review of security risks posed by Huawei and stated publicly that there was no clear evidence that Huawei had spied for the Chinese government.

The most significant risks were the presence of vulnerabilities in Huawei's equipment, a danger found in almost all information technology hardware and software devices and applications. While the company should be required to fix as many vulnerabilities as possible – as should any IT vendor selling technological solutions – sloppy equipment does not an espionage effort make. If so, then Microsoft would be singled out as the single greatest facilitator of espionage activity on the planet.

Threat or Not, Countries Still Work With Huawei

Huawei is the second largest telecommunications provider in the world, with deployed products and solutions in over 140 countries, indicating that the majority of the countries in the world do not fear Huawei as an intelligence threat. In 2011, Huawei's enterprise business experienced rapid growth, with its sales revenue reaching CNY9,164 million, a year-on-year increase of 57.1%. Sales increased 60.8% year-on-year when adjusted for currency exchange rate effects. This growth was attributable mainly to expanded offerings in Huawei's overseas markets. [13] Huawei has set up 23 research centers in Germany, Sweden, the UK, France, Italy, Russia, India, China, and other countries, according to the company's website.[14]

- The United Kingdom (UK), one of the United States greatest partners and closest allies, shares equal security concerns about Huawei. The UK established an independently managed Cyber Security Evaluation Center that conducts independent reviews of Huawei's equipment and software deployed to the UK's telecommunications' infrastructure.[15]
- In 2012, in an effort to achieve transparency, Huawei offered Australian authorities unrestricted access to its code and hardware to prove that it's not a threat.[16] In 2013, Huawei supported the creation of an Australian Cyber Security Center development to test the security credentials being implemented into critical infrastructure.[17]
- U.S. companies, particularly those in IT, continue to invest in China despite the alleged "intelligence" threat. Dell,[18] Intel,[19] Hewlett Packard,[20] Boeing,[21] and General Electric[22] are intending to substantially invest in China over the next years.

Conclusion

The United States used to be on the forefront of IT development, manufacturing, and services. With globalization, the U.S. opted to favor outsourcing as a means of spurring industry growth and profits, and consequently, fostered dependence on an international supply chain. A national strategy to address this concern has been formed by the White House, but is it needed?

Several elements need to be factored into national strategies such as milestones, performance measures, cost and resources, and roles and responsibilities, to name a few. All of this requires a significant investment in time, personnel, financial backing, policy development, oversight, accountability metrics, compliance penalties, etc., across public and private domains to address a threat that is just too large and too decentralized to mitigate effectively.

Risk can be managed, and every effort should be made to verify and validate IT equipment used by our critical infrastructures and national security apparatus. Similar programs like the one instituted in the UK addresses these very concerns and demonstrate how collaboration with an IT vendor would work. The benefits are substantial and mutual. For the customer, such partnering will aid in the immediate detection of defective or poor quality equipment prior to its implementation into key networks, thus ensuring the confidentiality, integrity, and availability of original equipment. For the vendor, rigorous testing information is supplied to product engineers bolstering their abilities to make stronger, more durable products. However, this is only possible by embracing these types of partnerships, not hiding from them.

If the U.S. wants to levy policies to enforce an economic protectionism, then so be it. It is entirely within their right to say they don't want Chinese companies to gain a niche in their market. But it shouldn't hide behind national security as an excuse for these economic policies, nor should it send mixed messages to Beijing that repeat how China is a partner and welcomed to invest in all things American.[23] The United States encouraged the very globalization that it now sees as a threat. If the U.S. fears companies like Huawei, then the government needs to be transparent and public with its findings. If not, it risks losing out on opportunities to strengthen its position as a global partner as well as proactively helping to strengthen the very networks it's worried about being compromised.

References

[1] Dancho Danev, "China's 'secure' OS Kylin - a threat to U.S offensive cyber capabilities?" Zdnet, May 13, 2009, accessed at: http://www.zdnet.com/blog/security/chinas-secure-os-kylin-a-threat-to-u-s-offensive-cyber-capabilities/3385

[2] Ellyne Phneah, "India Developing own OS to Boost Cybersecurity," *ZDnet*, December 21, 2012, accessed at: http://www.zdnet.com/in/india-developing-own-os-to-boost-cybersecurity-7000009118/

[3] John E Dunn, Paranoia Drives Iran to Develop Homegrown Antvirus Program," TechWorld, May 3, 2012, accessed at: http://news.techworld.com/security/3355680/paranoia-drives-iran-to-develop-homegrown-antvirus-program/

[4] Ryan Whitwam, "Russia to Create National Operating System," Maximum PC, October 27, 2010, accessed at: http://www.maximumpc.com/article/news/russia_create_national_operating_system

[5] Isha Suri,"Iran to Establish Its Own Cyber Defense Headquarters," Silicon Angle, July 25, 2012, accessed at: http://siliconangle.com/blog/2012/07/25/iran-to-establish-its-own-cyber-defense-headquarters/

[6] Government Accountability Office, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," GAO-12-361, March 2012, accessed at: http://www.gao.gov/assets/590/589568.pdf

[7] Carnegie Mellon University, Software Engineering Institute, "Evaluating and Mitigating Software Supply Chain Security Risks," CMU/sei-2010-tn-016, May 2010, p. 16, accessed at: http://www.sei.cmu.edu/reports/10tn016.pdf

[8] Government Accountability Office, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," GAO-12-361, March 2012, accessed at: http://www.gao.gov/assets/590/589568.pdf

[9] Government Accountability Office, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," GAO-12-361, March 2012, accessed at: http://www.gao.gov/assets/590/589568.pdf

[10] "Emerging Cyber Threats Report 2013," Georgia Tech Institute of Technology, accessed at: http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf

[11] General Accountability Office, "IT Supply Chain," GAO-12-361, March 2012, accessed at: http://www.gao.gov/assets/590/589568.pdf

[12] Jason Dedrick and Kenneth L. Kraemer, "Globalization of Innovation: The Personal Computing Industry," Alfred P. Sloan Foundation, Industry Studies 2008, accessed at: http://web.mit.edu/is08/pdf/Globalization%20of%20Innovation%20PC.PDF

[13] Huawei, "Huawei Investment Holding Co., Ltd. 2011 Annual Report," accessed at: http://www.huawei.com/ucmf/groups/public/documents/attachments/hw_126991.pdf

[14] Huawei Website, "Research and Development," accessed at: http://www.huawei.com/en/about-huawei/corporate-info/research-development/index.htm.

[15] U.S. House of Representatives; "Investigative Report on the U.S. National Security Issues posed by Chinese Telecommunications Companies Huawei and ZTE," October 8, 2012, accessed at: http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf

[16] Lisa Vaas, "National Security Threat or Not? Huawei Offers Australia Unrestricted Access to Code," NakedSecurity.com, October 25, 2012, accessed at: http://nakedsecurity.sophos.com/2012/10/25/huawei-australia/

[17] Hafizah Osman, "Huawei Supports Australian Cyber Security Centre Development," Arnnet.com, January 23, 2013, accessed at: http://www.arnnet.com.au/article/451519/huawei_supports_australian_cyber_security_centre_development_/

[18] China Daily, December 15, 2010, "Dell to Double Investment in China to $250b by 2020," accessed at: http://www.chinadaily.com.cn/business/2010-12/15/content_11704983.htm

[19] Aaron Back, April 12, 2012, "Intel, China's Tencent to Join on R&D," Market Watch, accessed at: http://www.marketwatch.com/story/intel-chinas-tencent-to-join-on-rd-2011-04-12

[20] China Economic Review, June 30, 2011, "HP Announces R&D Expansion in China," accessed at: http://www.chinaeconomicreview.com/content/hp-announces-rd-expansion-china

[21] Navjot Kaur, March 15, 2012"Boeing's Baby Steps in China," The Motley Fool, accessed at: http://www.fool.com/investing/general/2012/03/15/boeings-baby-steps-in-china.aspx

[22] Ying Wang and Rachel Layne, November 9, 2010, "General Electric Plans to Invest $2 Billion in China," Bloomberg, accessed at: http://www.bloomberg.com/news/2010-11-09/general-electric-to-spend-2-billion-on-china-technology-finance-ventures.html

[23] Department of Treasury, May 3, 2011, "Treasury Secretary on US-China Strategic and Economic Dialogue," accessed at: http://iipdigital.usembassy.gov/st/english/texttrans/2011/05/20110505191406su0.2003072.html#axzz2NRFDOhGG