The Heritage Foundation

BACKGROUNDER

No. 2880 | MARCH 6, 2014

Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace

David Inserra and Steven P. Bucci, PhD

Abstract

The many cybersecurity challenges facing the U.S. include one of which many Americans are unaware—the serious threat posed by vulnerabilities in the cyber supply chain. Of the many components—including hardware, firmware, and software—that compose a technological product, most contain elements stemming from a broad global market, making it difficult to ascertain the complete security of an end product. With the market for technological goods and components continuing to grow every year, and with everything from missiles to smartphones relying on these products, the need for cyber supply chain security has never been more important. It is essential that enhancing the security of the United States' technological supply chain not destroy the well-functioning international market for technology. Instead of the two extremes of intrusive government mandates or doing nothing, the U.S. government should promote development of a private-sector system for securing and accrediting technology companies that would allow customers—from the federal government to small businesses—to make more informed and risk-based decisions.

The many cybersecurity challenges facing the U.S. include one of which many Americans are unaware—the serious threat posed by vulnerabilities in the cyber supply chain. Of the many components—including hardware, firmware, and software—that compose a technological product, most contain elements stemming from a broad global market that includes nations as diverse as Germany,

Key Points

- Many cybersecurity challenges face the U.S.—including one of which many Americans are unaware: the serious threat posed by vulnerabilities in the cyber supply chain.
- Of the many components that make up a technological product, most contain elements from a broad global market, making it difficult to ascertain the complete security of an end product.
- With the market for technological goods and components growing every year, the need for cyber supply chain security has never been greater.
- Any effort to enhance the security of the United States' technological supply chain must not destroy the well-functioning international market for technology.
- Instead of the two extremes of intrusive government mandates or doing nothing, the U.S. government should promote a private-sector system for securing and accrediting technology companies that would allow customers of all sizes and from all industries to make more informed and risk-based decisions.

This paper, in its entirety, can be found at **http://report.heritage.org/bg2880**

Produced by the Douglas and Sarah Allison Center for Foreign and National Security Policy

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

China, India, Brazil, and Japan, as well as many others, making it difficult to ascertain the complete security of an end product. With the market for technological goods and components continuing to grow every year, and with everything from missiles to smartphones relying on these products, the need for cyber supply chain security has never been more important.

It is essential that any effort to enhance the security and integrity of the United States' technological supply chain not destroy the well-functioning international market for technology. This market allows companies to purchase inexpensive components and then sell their products at lower cost to U.S. and international electronics consumers. Instead of the two extremes of intrusive government mandates or doing nothing, the U.S. government should promote development of a private-sector system for securing and accrediting technology companies that would allow customers of all sizes and from all industries to make more informed and risk-based decisions.

Understanding the Cyber Supply Chain

The growth and power of technology has led to increased demand for technology products. In the U.S., the number of households with at least one personal computer (PC) increased from 71.1 percent in 2008 to 81.3 percent in 2013. Even more telling, international smartphone sales surged 42.1 percent from 2011 to 2012.[1] As a result of the growing use of and demand for technological products, the industries that supply them have also grown and expanded internationally.[2]

Increased demand has led to acute competition and, consequently, more outsourcing and innovation to lower costs and remain competitive. This can be seen in the U.S. computer manufacturing sector, which over the past five years has declined at an annual rate of 21.8 percent as computer manufacturing has increasingly moved abroad.[3] On the other hand, software, information technology services, and computer-chip development are growing and diversifying markets within the U.S. as thousands of companies seek to service the growing number of computer products, provide innovative and useful software applications, and power the next generation of computers with faster chip designs.[4] Of course, the expanding market for these goods means that even these industries are seeing international competition and outsourcing that will likely grow over time.[5]

When talking about the supply chain for technology and computer products it is important to understand the different types of products. The three major elements of any computer as well as many other technology products are:

- **Hardware**, including computer chips, which process and complete the work needed to perform a given task;
- **Firmware**, which is the essential, embedded software needed for basic hardware operation; and
- **Software**, the computer programs that task the hardware with specific activities and tell it how to complete those activities to yield a certain result.

The expansive and international field of technology suppliers means that each of these elements is often created from pieces of many different com-

1. News release, "Strong Demand for Smartphones in Second Quarter Continues to Drive the Worldwide Mobile Phone Market, According to IDC," International Data Corporation, July 26, 2012, http://www.idc.com/getdoc.jsp?containerId=prUS23624612 (accessed October 15, 2013).
2. OECD, *OECD Internet Economy Outlook 2012*, 2012, http://www.keepeek.com/oecd/media/science-and-technology/oecd-internet-economy-outlook-2012_9789264086463-en (accessed October 15, 2013).
3. IBISWorld, "Computer Manufacturing in the US: Market Research Report," December 2013, http://www.ibisworld.com/industry/default.aspx?indid=740 (accessed January 7, 2013).
4. "The Software and Information Technology Services Industry in the United States," SELECTUSA, http://selectusa.commerce.gov/industry-snapshots/software-and-information-technology-services-industry-united-states (accessed October 15, 2013); "Semiconductors," SELECTUSA, http://selectusa.commerce.gov/industry-snapshots/semiconductors (accessed October 15, 2013); IBISWorld, "Software Publishing in the US: Market Research Report," October 2013, http://www.ibisworld.com/industry/default.aspx?indid=1239 (accessed October 15, 2013).
5. IBISWorld, "Global Semiconductor & Electronic Parts Manufacturing: Market Research Report," August 2013, http://www.ibisworld.com/industry/global/global-semiconductor-electronic-parts-manufacturing.html (accessed October 15, 2013).

panies. For example, a computer chip might need to fulfill several functions, including visual, audio, and transmission capabilities. Three or more companies could be contracted to complete work on specific parts of the chip, since some companies are better at, and less expensive at, working on visual parts of the chip, while others are better at making audio or transmission parts. This outsourcing or contracting process is also used for writing software and firmware computer codes. Given the vast number of hardware, firmware, and software components and subcomponents needed for thousands of different electronics products, such contracting and subcontracting is necessary to produce affordable and cutting-edge technology.

This process is evident in the creation of an iPhone. Companies from the U.S., South Korea, Taiwan, Japan, Germany, and elsewhere provide components, many of which contain other international components, which are then assembled in China.[6] Indeed, Apple buys parts from over 200 suppliers and manufacturers around the world to create its products.[7] While any of the foreign companies could be replaced by an American one, cost, flexibility, or speed would be sacrificed by doing so. The highly international supply chain helps Apple, as well as other technology companies, create innovative and relatively inexpensive products.

Supply Chain Under Attack

While the diversity within the technology industry enables innovation and low prices, it also increases the chances of tainted, counterfeit, and malicious goods entering the market. Of course, sometimes vulnerabilities in technology are simply design mistakes in a piece of hardware or gaps in software and firmware coding. But, whether malicious or not, vulnerabilities in the supply chain can be—and often are—used for malicious ends, be it cyber attacks or espionage.

Regarding software, a March 2013 study by the International Data Corporation found that "at least a third of all PC software is counterfeit."[8] Counterfeit software both directly and indirectly threatens the security of the user. It directly affects the security of the user since malicious software, called malware, is often attached to the counterfeit software. It can be preinstalled on a computer or downloaded by a user. Indirectly, counterfeit software can compromise security by requiring the user to visit dangerous websites to download or authenticate a product. Furthermore, many counterfeit products, even if not malicious, cannot be as easily updated or patched to correct vulnerabilities and flaws, leading to less security in the long run.

As a result of counterfeit software, most users experience decreased computer performance, viruses, spam, or complete failure of the software or computer. Dealing with infected software is estimated to cost the world more than $100 billion annually, while the indirect costs related to data losses and identity theft could cost another $350 billion.[9] While too few studies exist to fully analyze the international scope of this problem, clearly software counterfeiting is a serious and costly cybersecurity threat.

The same is true of hardware threats, which are even more difficult to identify and remedy. Malicious hardware may contain special back doors that are difficult to detect when tests are performed. Dr. John D. Villasenor, an expert at the Center for Technology Innovation at the Brookings Institution, encapsulates this problem well:

> Consider the following example: Suppose that a company outsources the design for a block of the chip that is supposed to add the number six to any input. During testing, if 20 is provided to this block, the block outputs 26. When 127 is provided, the block outputs 133. One hundred thousand more inputs are provided, and in every case,

6. Yuping Xing and Neal Detert, "How the iPhone Widens the United States Trade Deficit with the People's Republic of China," Asian Development Bank Institute *Working Paper* No. 257, December 2010, revised May 2011, (accessed October 15, 2013), and Alex Hillsberg, "How and Where iPhone Is Made: A Surprising Report on How Much of Apple's Top Product is US-Manufactured," FinancesOnline, http://financesonline.com/how-iphone-is-made/ (accessed October 15, 2013).
7. Apple Incorporated, Supplier List 2013, January 2013, http://images.apple.com/supplierresponsibility/pdf/Apple_Supplier_List_2013.pdf (accessed October 15, 2013).
8. John F. Gantz et al., "The Dangerous World of Counterfeit and Pirated Software," International Data Corporation *White Paper*, March 2013, http://www.microsoft.com/en-us/news/download/presskits/antipiracy/docs/idc030513.pdf (accessed October 15, 2013).
9. Ibid., p. 23.

> the result comes back correct. This block will be deemed to have passed functional testing. But the block could have a hidden circuit triggered by an input with value 126,321,204. When that input—and that input alone—arrives, an attack is launched. Because testing can't possibly be exhaustive, this input will never be encountered until it is provided months later by an attacker.[10]

In addition to making pre-use testing problematic, malicious and counterfeit hardware may also be more difficult to identify once an attack takes place. Hardware failure or malware would likely be suspected before malicious hardware, especially since diagnostic tests as described above might not find the malicious circuit. While the Defense, and Intelligence, Advanced Research Projects Agencies (DARPA and IARPA respectively), are working on ways to analyze chips for counterfeiting and tampering, this research is still in the works and will likely never be a complete solution.[11]

Such testing and detection difficulties make malicious hardware particularly dangerous. The hardware could be automatically activated, or it could wait for a command or a certain date or location. Once activated, malicious hardware can covertly siphon off communications and information transiting the system. The hardware could also become corrupted, or simply cease to function.[12] Malicious hardware could also open a backdoor for malware, further compromising a computer or network, while obscuring the underlying hardware threat.

While malicious hardware can have serious financial impacts on U.S. businesses, it is especially worrisome for U.S. military systems. In October 2011, two people were convicted of selling as many as 59,000 counterfeit circuits from China to the U.S. military, defense contractors, and others for use in U.S. warships, airplanes, missiles, and missile defense systems.[13] Not only were these cheap fakes, but these chips potentially contained serious vulnerabilities that could have disabled, impaired, or stolen information from these important systems. This example is just one of many known cases of counterfeit hardware, not to mention those cases where counterfeit hardware slipped through. The Commerce Department reported a doubling of counterfeit incidents with the military and its suppliers between 2005 and 2008, to more than 9,356 cases.[14] As a more recent Government Accountability Office (GAO) report has found, while the Defense Department has taken measures to protect its supply chain, counterfeit and potentially malicious hardware is most likely still finding its way into critical systems.[15]

If a piece of malicious or counterfeit hardware is suspected, it is also potentially more troublesome to replace. The specific chip or computer board threat must first be identified and then replaced. When malware or counterfeit software is discovered, the solution is a detailed virus scan, uninstallation of a program, or the replacement of a program with a legitimate version. When malicious hardware is discovered, a technician must physically remove the offending hardware and replace it with a new, more secure, piece of hardware. Other machines with similar hardware must also be tested, and the hardware must also be replaced.

10. John Villasenor, "Ensuring Hardware Cybersecurity," The Brookings Institution, May 2011, http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity (accessed October 15, 2013).
11. Robert Johnson, "The Navy Bought Fake Chinese Microchips that Could Have Disarmed U.S. Missiles," Business Insider, June 27, 2011, http://www.businessinsider.com/navy-chinese-microchips-weapons-could-have-been-shut-off-2011-6 (accessed October 14, 2013), and Adam Rawnsley, "Fishy Chips: Spies Want to Hack-Proof Circuits," *Wired*, June 24, 2011, http://www.wired.com/dangerroom/2011/06/chips-oy-spies-want-to-hack-proof-circuits/ (accessed October 15, 2013).
12. Villasenor, "Ensuring Hardware Cybersecurity."
13. William R. Levesque, "Pinellas Woman Gets 38 Months in Prison in Counterfeit Electronics Case," *Tampa Bay Times*, October 26, 2011, http://www.tampabay.com/news/courts/criminal/pinellas-woman-gets-38-months-in-prison-in-counterfeit-electronics-case/1198637 (accessed October 15, 2013).
14. Spencer S. Hsu, "U.S. Charges Florida Pair with Selling Counterfeit Chips from China to the U.S. Navy and Military," *The Washington Post*, September 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/14/AR2010091406468.html?nav=rss_business/industries (accessed October 15, 2013).
15. Government Accountability Office, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," *Report to Congressional Requesters*, March 2012, http://www.gao.gov/assets/590/589568.pdf (accessed October 15, 2013).

These threats, both through software and hardware, are a concern to all actors. Private industry can experience poor computer performance, leaked business plans, and the legal costs of data breaches. The government and military fear these effects, as well as many others, such as the disabling or impairing of critical military systems and weapons, including global positioning systems, missiles, and communications systems. Indeed, multiple reports from the GAO, the House Permanent Select Committee on Intelligence, and other government sources have warned of the threat of malicious hardware and software in U.S. government computer systems.[16]

Grading the Supply Chain Security of Technology Companies

Given the very real threat to America's economy and national security, the U.S. must secure its cyber supply chain, and must do so without harming the innovation-spurring and cost-saving nature of the global technology marketplace. To do so, the U.S. should adopt a private sector–driven system of supply chain security ratings, similar to how Underwriters Laboratories certifies the safety of electronic devices.

Such a system would operate by accrediting the supply chain security practices and procedures of participating companies. The Open Group, a technology consortium dedicated to improving business through IT standards, has established the Open Trusted Technology Provider Standard and Framework (O-TTPS and O-TTPF, respectively) which Congress should adopt. O-TTPS is a collaborative, business-developed list of flexible, technology-neutral, and continually updated best practices for supply chain security. A company seeking accreditation must determine how to minimize risk through best practices or similar efforts per the O-TTPS. The O-TTPS includes a spread of security issues including understanding and verifying the safety of components from upstream suppliers; control and supervision of in-house design and production; oversight of downstream users and delivery methods; and many other elements.[17]

Companies will then submit to various levels of evaluation as described by the O-TTPF. The levels of evaluation of a company's supply chain security are:

- Tier A: Self-Assertion and Third-Party Administration;
- Tier B: Third-Party Accreditation; and
- Tier C: Third-Party Accreditation of Specific Products.[18]

These levels of accreditation provide different levels of security as the sellers of technology see necessary. A well-known organization might not feel that it is necessary to undertake a product-level examination of its supply chain procedures. A relatively unknown technology company would likely want to prove the integrity and security of its products by undertaking a greater degree of scrutiny.

Such a system provides extra information that consumers can use to make risk-based decisions. For example, when choosing between two suppliers of equal reputation, a company with a Tier B or Tier C ranking will likely be more secure than a Tier A or unrated company. Indeed, a company with a proven and accredited supply chain will likely be able to charge more or command greater respect for its goods, giving technology companies a profit incentive to participate in the O-TTPF. Of course, consumers could also choose to buy from less secure companies if the product will be used for relatively non-sensitive or unimportant purposes, or if the company cannot afford to purchase products with the highest levels of accreditation.

16. Ibid., and Mike Rogers and C. A. Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," Permanent Select Committee on Intelligence, U.S. House of Representatives, October 8, 2012, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf (accessed October 15, 2013).
17. The Open Group Trusted Technology Forum, "Open Trusted Technology Provider Standard (O-TTPS)™ Version 1.0: Mitigating Maliciously Tainted and Counterfeit Products," April 2013, p. 6.
18. The Open Group Trusted Technology Forum, "Open Trusted Technology Provider Framework: Industry Best Practices for Manufacturing Technology Products that Facilitate Customer Technology Acquisition Risk Management Practices and Options for Promoting Industry Adoption," February 2011, pp. 20–21. Administration merely ensures that the company that self-asserts its compliance has completed and filed the proper compliance documents; accreditation requires that a third party review the contents of the compliance documents.

The O-TTPF will require third-party evaluators to confirm that a company has met the accreditation standards, with different levels of inspection depending on the tier. The evaluators, however, will need to follow a specific program to ensure that they are accurately accrediting organizations' supply chains. To this end, Open Group is developing a clear conformance program that all evaluators will use to review companies' supply chain procedures.[19] Such a program will allow sellers to certify their compliance with supply chain standards as well as enable Open Group to ensure that third-party evaluators are doing their work correctly. Additionally, while the government should not be responsible for establishing the standards or running this system, continual government cooperation with Open Group will ensure that this program works effectively.

While the Open Group system need not be the exact standard and framework that is promoted by Congress, it lays out a compelling and useful model for how to structure a cyber supply chain accreditation system.

Special Cases

In addition to cyber supply chain rankings, there are a few select supply chain issues that the U.S. must address. The first is the role that China's government and Chinese companies play in the supply chain and provision of technological components; the second is assuring resilience in national security computer systems.

China is a known bad cyber actor that considers its telecommunications industry to be an area of absolute state control.[20] Chinese telecom companies, such as Huawei and ZTE, are increasingly active on the world stage, selling telecommunications hardware and infrastructure. These companies could plant or know of serious flaws in the infrastructure they sell. While many companies such as ZTE are simply state-owned, others, like Huawei, claim some level of independence from the Chinese government. Given that the Chinese government considers telecommunications to be an area of absolute state control and the Chinese government controls all avenues of legal recourse, no Chinese company can reject demands from the government for information on vulnerabilities in other's systems. As a result, the Chinese government likely already has or could at any point ask for information about cyber vulnerabilities to further economic espionage or military exploitation.

Given such concerns, the House Permanent Select Committee on Intelligence's report on ZTE and Huawei recommended that they not be considered as partners on projects involving sensitive systems.[21] This recommendation is worth heeding when dealing with areas vital to U.S. national security. The Department of Homeland Security (DHS) and the Defense Department should build on and update existing acquisition rules to ensure that sensitive systems are properly defended from supply chain risks. When dealing with systems not critical to national security, which is the vast majority of the U.S. economy, however, the private sector should be free to work with Chinese telecommunications companies if they feel such actions to be a wise business decision.[22]

On the other hand, U.S. builders of military and other critical systems may consider built-in chip defenses in their hardware. To prevent malicious hardware from completing an attack, chips can be equipped with a small amount of circuitry that monitors how a chip is functioning, identifies and isolates any malicious activity, and then informs similar devices about the potential threat.[23] Such a safety net, of course, requires that the monitoring circuits come from a trusted source. A DHS and Defense Department policy that identifies critical systems and adds redundant and warning systems will make security systems more resilient and less vulnerable to a devastating hardware attack.

For less critical government systems and the private sector, cloud computing could be another way

19. The Open Group Trusted Technology Forum, "Open Trusted Technology Provider Standard (O-TTPS)™ Version 1.0: Mitigating Maliciously Tainted and Counterfeit Products," p. 3.
20. Derek Scissors and Steven P. Bucci, "China Cyber Threat: Huawei and American Policy Toward Chinese Companies," Heritage Foundation *Issue Brief* No. 3761, October 23, 2012, http://www.heritage.org/research/reports/2012/10/china-cyber-threat-huawei-and-american-policy-toward-chinese-companies.
21. Rogers and Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications."
22. Scissors and Bucci, "China Cyber Threat."
23. Villasenor, "Ensuring Hardware Cybersecurity."

to reduce supply chain risks and encourage resilience in the event of an attack. Except for the device accessing the cloud, cloud service providers (CSPs) manage the security and integrity of hardware, new software, and software updates for cloud users. These CSPs are better able to deal with security concerns than many individual companies can on their own. Furthermore, if a company's computers were infected or disabled by a cyber attack, that company could easily access its cloud service through uncompromised devices. Instead of losing access to important data, applications, and functionality while the damage from the cyber attack is repaired, cloud users would quickly have access to data and applications via a cloud server.[24]

Defending the International Marketplace for Technology

The threat of counterfeit and corrupted hardware and software requires real solutions that enhance security without destroying the incredibly effective international supply chain. Therefore, Congress and the Administration should:

- **Encourage the private development of cybersecurity supply chain ratings and accreditation.** These ratings should be based on a private-sector set of best practices like the O-TTPS, and operate via a framework similar to the O-TTPF. Such a framework would contain different tiers or ratings for different levels of accreditation, ranging from minimal overview of a company's supply chain to in-depth analysis of specific products' supply chain features. These different levels of accreditation will provide consumers with more information, with which they can make better, risk-based decisions. Additionally, producers will find such accreditation valuable for selling their products, thus connecting security and a profit incentive. Instead of mandating cybersecurity solutions, the U.S. government should collaborate with the private sector. A specific way to encourage the adoption of this system would be to require government agencies that deal with large amounts of sensitive data, or have security-related duties, to purchase technology only from organizations that are accredited by this cyber supply chain ratings system.

- **Improve sensitive government and military cyber supply chain procedures.** GAO reports and news accounts indicate that the government needs to improve its supply chain procedures for technology products. Such improvements should include the requirement that no technology be purchased from Chinese companies for use in U.S. national security systems. Additionally, government agencies should be required to consider supply chain ratings when purchasing technology goods and integrate relevant portions of O-TTPS into their acquisition processes.

- **Enhance cyber resilience.** In critical government systems, hardware that monitors itself for hardware attacks and other redundancies should be considered. Though likely more expensive, the U.S. should recognize this premium as a way to protect its most important systems. For agencies with less sensitive systems, the U.S. should consider expanding cloud computing to gain access to rapidly scalable and quickly available computer resources as a way to enhance resilience and continuity of operations at low cost.

Cyber Supply Chain Security: Too Important to Be Ignored

The U.S. has enjoyed the benefits of a global marketplace and supply chain for technological products, including lower prices and increased opportunities for innovation. These benefits have not come without cost, however, and the risk of compromised hardware, firmware, and software is serious. The U.S. should deal with this risk by promoting a private sector–led system of cyber supply chain ratings that will enhance the integrity of technological products, provide customers with more information with which they can make better risk-based decisions, and thus tie supply chain security to businesses' profit motive. Along with other commonsense reforms to government cyber systems and

24. Steven. P. Bucci, "Getting Cyber Serious: Mastering the Challenges of Federal Cloud Computing," Heritage Foundation *Backgrounder* No. 2705, June 27, 2012, http://www.heritage.org/research/reports/2012/06/getting-cyber-serious-mastering-the-challenges-of-federal-cloud-computing?ac=1.

supply chains, the U.S. can mitigate the risk of compromised cyber products, increase cyber resilience, and enjoy the benefits of the cyber marketplace.

*—**David Inserra** is a Research Assistant for National Security and Cyber Security in, and **Steven P. Bucci, PhD,** is Director of, the Douglas and Sarah Allison Center for Foreign and National Security Policy, a department of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*