The China Syndrome

The Huawei security risk: Factors to consider before buying Chinese IT

By Joel Snyder (jms@opus1.com)

This article appeared in Information Security magazine in February, 2013, and is reprinted with permission.

Globalization has reduced competitive barriers between both multinational corporations and nation states. For an IT professional struggling to decipher a routing protocol error code or configure a firewall, the international nature of technology is a boon: be it in Boston, Brussels, Bogota, Brazzaville or Baku, someone somewhere has the product, service or information that an IT organization may need to run more smoothly or securely. However, the increasingly flat world isn't to everyone's taste.

Globalization has also created a collision of diverse interests in the world of technology, emphasizing layers 8, 9, and 10 of the ISO network model: the political, religious and economic layers. In the information security realm, those interests collided dramatically in 2006, when Israeli security vendor Check Point Software Technologies Ltd. attempted to buy U.S.-based vendor Sourcefire Inc. for $225 million, but the deal was scuttled by the Committee on Foreign Investment in the United States, a little-known U.S. government committee. CFIUS, in turn, was reacting to political backlash from its earlier approval of a sale of 22 U.S. port operations from a British company to a UAE company, a decision congressmen from both sides of the aisle denounced.

Just last year, an even more dramatic confrontation led to the two largest Chinese telecommunications equipment manufacturers, Huawei Technologies Co. Ltd. and ZTE Corp., being demonized by the U.S. House of Representatives Permanent Select Committee on Intelligence for providing "incomplete, contradictory, and evasive responses to the Committee's core concerns" during its year-long investigation into the threat they pose to U.S. interests. Although the Committee found no concrete evidence of wrongdoing, it called the two companies a threat to U.S. national security and suggested they be effectively kicked out of the U.S. telecommunications market and investigated for unfair trade practices.

While network managers in government agencies may have no choice but to cross Huawei and ZTE off their purchasing lists in response to the House's concerns, both vendors are highly motivated to make inroads in the U.S. IT market and have shown a willingness to price their products aggressively. For that reason alone, private sector IT staff have an opportunity, if not an obligation to take a reasoned approach, weighing the risks and mitigations involved, when deciding whether to buy Chinese IT.

Who's Really Chinese?

It's worthwhile to consider what it means to "buy Chinese." Obviously, companies like Huawei, which have tight ties to the Chinese government and operate by Chinese business and intellectual property rules, represent a point at one end of the spectrum.

But the Chinese are major players in the supply chain of virtually every telecommunications product produced today, providing manufacturing and assembly facilities to vendors around the world. No piece of network equipment is manufactured without Chinese-sourced components, and a great deal of final assembly from major vendors such as Cisco Systems Inc., Juniper Networks Inc., Hewlett-Packard Co., Apple Inc. and Dell Inc. depend heavily on facilities in China.

In other words, every piece of networking and server equipment you buy is at least partially Chinese already.

What are the risks of buying Chinese?

There are four commonly mentioned threats associated with buying goods from Chinese companies such as Huawei, ranging from the imagined and unlikely to clear and serious business risks.

1) **The Magic Kill Packet:** Straight out of a Hollywood summer blockbuster, the Magic Kill Packet threat is that someone, somewhere, can cause network equipment to shut down by sending some special combination of ones and zeros. This magic kill packet would be sent during a real-world cyberwar involving China and, one supposes, everyone who bought Huawei equipment. (Huawei's domestic sales represent about a third of its total revenues.) [[See 2011 Annual Report, PAGE 11, Sales Revenue China = 65,565 CNY Overseas = 138,364 CNY. 32%]] While the idea of a Magic Kill Packet (and similar ticking time bomb threats) doesn't hold up to any serious analysis, it makes for good chatter in the blogosphere. Security and network managers who have to calm anxious senior managers can point out that the control plane for enterprise routers is always separate and firewalled from the data plane, so an attacker would already have to have cracked into your network. And a Magic Kill Packet at the data plane would also be nearly impossible to inject, given the heavy use of access control lists, firewalls and NAT in enterprises. There's no way a Magic Kill Packet could shut down entire networks, because each individual

device would have to be carefully targeted with a specifically engineered strategy to deliver the payload.

2) **Intentionally Bad Software**: This threat suggests that Chinese-manufactured devices have hidden back doors that would allow an attacker to gain special access. One example is a master password that allows an attacker to log into the device as an administrator at any time. For example, in 2003, Dave Tarbatt discovered that most manageable UPS backup devices made by American Power Conversion Corp. (APC) could be accessed with a secret factory default password, intentionally placed there by the APC. (Of course, the "A" in "APC" stands for "American," so this isn't just a Chinese issue.)

A more complicated version of the Intentionally Bad Software threat applicable to a Chinese vendor might include a hidden intentional bug that would allow an attacker access through some other path. For example, the SSH server in the device might be susceptible to a particular buffer-overflow attack. An intrusion exploiting this would seem like a typical zero-day attack. Of course, intentional bugs and master passwords would, like the magic kill packet, only work for a short period of time and for a few devices once the intrusion was detected.

Intentionally Bad Software in telecommunications hardware could also expose encrypted data in VPNs. If the random number generator used in an IPSec or SSL VPN device is not truly random, then an outsider who knows about the lack of randomness may be able to decipher data secured with even the most advanced encryption protocols, and no evidence of any tampering left behind. If an attacker can passively tap encrypted traffic, information disclosure could go on for years without anyone finding out.

Intentionally bad software—factory default passwords, known bugs that would allow access and defective random number generators—seem like plausible outcomes if one assumes that Chinese manufacturers are operating under direct instructions of the Chinese government or military.

Lke the Magic Kill Packet, these threats don't make a lot of sense. Since Chinese manufacturers also dominate the Chinese marketplace, any dangling backdoor intentionally left in network equipment would also be accessible to someone wanting to monitor Chinese communications. Chinese manufacturers, or their shadowy military puppet masters, couldn't risk installing a secret backdoor unless they were sure that only they could take advantage of it. And as groups like Anonymous and Wikileaks have shown us, even the best-kept secrets can quickly be revealed.

3) **Unintentionally Bad Software:** If intentional backdoors are unlikely, then what about plain old bugs? What about the possibility that critical infrastructure devices and servers have software or hardware errors in them that could possibly compromise the security of a network? Would that be a reason to knock a vendor off one's preferred suppliers list?

Of course, this question can only be asked in jest, because every single software, hardware and chip vendor has released products with bugs. Everyone knows it, and these bugs have created an entire industry. Most of the IT security world, including antimalware, vulnerability analysis, patch management and intrusion-prevention software, sprung up to compensate for the effects of lousy software, buggy hardware and poor configurations. If we all stopped buying from every vendor that has had security flaws in its products, we'd have a hard time moving beyond pencil and paper.

In the "intentionally bad software" category, we put "poor random number generators for VPNs." But poor random number generators happen accidentally all the time, sometimes with spectacular results. For example, early versions of the Netscape browser used only a 16-bit random number generator for SSL communications, making a brute-force attack on encrypted data simple even using the slowest computers. MIT's Kerberos key management system, now at the core of the Windows security architecture, had a random number generator with a key space limited to about 20 bits (about 1 million keys, easy to brute force), for nearly 10 years.

But it isn't fair to put, for example, Huawei in the same category as Cisco and Juniper when it comes to security awareness. Huawei claims to be a willing participant in the world of information security. On its website, Huawei says that it "… is willing to work with all governments, customers and partners through various channels to jointly cope with cyber security threats and challenges from cyber security."

However, while Huawei is talking the talk, it isn't exactly walking the walk. A combination of factors, including significant cultural and language issues, has kept Huawei from following the path of other vendors. We have come to expect responsible disclosure of security problems, prompt product updates for known issues, active participation in industry security forums and easy access to security-patched software images from our network and security product vendors. Huawei isn't up to snuff in any of these areas.

But this is an issue with a single vendor and completely transcends national boundaries. Yes, Huawei may be a poor bet for buggy software, but that's not because it's Chinese–-it's because Huawei behaves more like a bargain-basement , release-and-forget hardware vendor in the routing and switching space than a high-end security-focused networking company like Cisco, Juniper or HP.

In other words, the standard for choosing a network product vendor isn't necessarily the pattern on the flag above the company headquarters, but the way that the vendor participates in the worldwide information security community. Vendors who pay more than lip service to maintaining the security of their products are better equipped to serve the needs of enterprise users. Network and security managers considering the purchase of critical infrastructure must pay attention to these issues, no matter what the origin of the equipment.

4) **Business Issues:** Not every threat to network security has its origins in bad or malicious software and hardware. An important, non-technical issue when considering suppliers from China is the differing cultural frameworks for both competition and intellectual property. The Chinese government and political infrastructure requires that any successful company be intertwined with the Communist Party, which itself is integrated into the government and military infrastructure of the country. This is normal in China. As long as buyers are aware of this as a standard part of doing business with Chinese manufacturers, and act accordingly, there is no particular reason to worry about one Chinese supplier over another. Huawei's ties to the government and military are not a quiet conspiracy—this is just how big business happens in China.

However, the commingling of interests between Chinese companies and the Chinese government means that Chinese companies owe their first loyalty to China, and not necessarily to their customers. The implication of this loyalty structure is that network equipment buyers must be sure to engage in secure practices when working with all of their vendors. Many IT staff have come to regard equipment suppliers as trusted partners, offering broad access to help in troubleshooting and sharing sensitive information about network configurations and growth plans. Network and security managers dealing with Chinese companies should consider the different attitudes and loyalties of these companies, and maintain a healthy distance when it comes to sensitive information and access controls.

Company stability is another fair concern. If an enterprise standardizes on a product line and the product line disappears, this can cause a significant disruption and heavy management overhead. When 3COM abruptly exited the enterprise networking market in 2000 and when Nortel went bankrupt in 2009, hundreds of enterprise customers who had built their networks on 3COM and Nortel equipment incurred significant costs, and significant risks, with no real support or security patches available from either vendor.

There are a number of concerns worth mentioning that aren't specific to information security. One is company stability. Is there any way to really know if Huawei and ZTE will be around next year, supporting the products they're selling now? A related concern is a relative lack of transparency compared to most U.S. and European companies. When reports on company financials or even company ownership are unaudited or, in some cases, completely unavailable, cautious buyers may have little to validate their choices. Even when information is available, it may not be easy to compare Chinese companies with their competitors. Huawei and ZTE, as two of the largest telecommunications vendors in the world with tens billions of dollars in sales, seem to be strong companies, but it is impossible for a typical network manager—or US congressional committee—to say for sure.

Is There a Risk From Buying Chinese?

Much of the rhetoric surrounding Chinese companies such as Huawei is short on facts and long on xenophobia, motivated more by political and financial concerns than any substantiated threat. Network and security managers considering buying from Chinese companies should perform the same due diligence as with any vendor, considering product quality, support and their long-term viability prospects before committing to a significant purchasing decision. While Chinese companies do operate under a different set of business rules than their North American and European competitors, these differences simply serve as an important reminder to protect sensitive information and maintain an appropriate arms-length relationship, as with any service or equipment provider, regardless of which nation that vendor calls home.

About the author:
Joel Snyder is a senior partner with consulting firm Opus One in Tucson, Ariz. He has