It used to be a truism that the purpose of managing the supply chain was to ensure sufficient materials and parts so as to execute the program. The prime contractor won the work and subcontracted portions to lower-tier suppliers, who then subbed out some to the next tier of suppliers, and so on and so forth. Primes got graded on the socioeconomic status of their subcontractors, with competitive advantage being conferred to those primes who could locate suppliers that were both good at execution and at being the right shade of socioeconomic category. The same was true for the lower-tier suppliers. If you could quote a decent price plus be a small or small disadvantaged business, you had a decent chance at winning work and making some money along the way.

The decision to subcontract out a portion of the contract's statement of work – the "make or buy" decision – was based on many factors, perhaps chief among them the notion that suppliers were generally smaller companies with less overhead—and thus cheaper. Often, there were other factors that also went into the make or buy decision. Some suppliers offered technical expertise unavailable to the prime contractor. Other suppliers offered the ability to promise good socioeconomic stats. Still other suppliers (often competitors) offered something even more valuable: the ability to deliver the political capital necessary to keep the program of record funded. To sum up a complex trade-off analysis in one sentence, the make or buy decision often pointed to a "buy"—a decision to subcontract out—even if the decision introduced additional program execution risk.

We've written about effective subcontractor management many times on this blog. For example, see **this article**, written about a year ago. Or see **another example**, written in 2010. We've asserted (with evidence in support of the assertion) that effective subcontractor management is the key to effective program management. We've written about the risks associated with subcontracting and the importance of identifying and managing those risks. We're kind of passionate about the topic, you might say.

Many of the largest prime contractors have made a specialty of subcontracting out large portions of the SOW, to the point where they like to call themselves “system integrators” and point to subcontract management as one of their (few) core competencies. Their program win strategy is to lock-up and deliver large teams of individual corporations (along with those corporations’ local Congresspersons and Senators). And it tends to work for them often enough that they keep on doing it. Either they have figured out how to manage the risks associated with supply chain management or, perhaps, they haven’t noticed that those risks keep increasing … and so they keep on with what has been working for them.

But make no mistake, those risks *do* keep increasing. We’ve written about those more recent risks, and the need to manage them, as well. Hell, we’ve even
ranted
about the importance of a secure supply chain more than once on this site, not that you took us seriously enough to mobilize a tiger team to attack the problem. For example, remember
that time
where we told readers about the revisions to the DFARS that established criteria for a contractor system to detect and avoid counterfeit electronic parts (“CEPDAS”)? It wasn’t that long ago: it was posted in May, 2014. Yeah, that was the one where we noted that a failure to implement an adequate CEPDAS could lead to a disapproved Purchasing System. That wasn’t the entirety of the risk.

In that article, we noted the new DFARS Cost Principle at 231.205-71, which made the cost of counterfeit electronic parts “and the cost of rework or corrective action” necessary to remedy the impacts of counterfeit electronic parts unallowable, unless the contractor has an approved CEPDAS (among other criteria). If you don’t have an approved CEPDAS and your supplier delivers counterfeit electronic parts, you are going to be in a world of financial hurt, hurt which you will only hope will be recoverable through litigation against your supplier.

This is a supply chain management risk and it’s a big risk and it’s hard to mitigate. Thus, since 2014 the make or buy decision has been impacted and we bet not too many companies have revised their make or buy processes and trade-off criteria accordingly. If you are one of the few who are out in front of this issue, then good for you! If not, you may want to read the next part of this article.

We now link to a very recent Department of Justice **press release** , in which we learn that Mr. Jeffrey Krantz, CEO and owner of Harry Krantz, LLC, a New York company “that bought

and sold, among other things, obsolete electronic parts for use by the U.S. Military and commercial buyers," pleaded guilty to one count of wire fraud. What did Mr. Krantz and his company do? According to the press release, Krantz did the following –

Between 2005 and 2008, KRANTZ purchased and sold, and caused to be purchased and sold, over a thousand chips to Bay Components, which, in turn sold them to the Connecticut company. The chips were marked with certain information, including a certain manufacturer's name and trademark, a date code, and a military part number. In approximately December 2005, the first shipments of about 330 chips that KRANTZ had sold to Bay Components were rejected by the Connecticut company for being the wrong part because the chip contained the wrong die inside. In 2006, KRANTZ replaced those chips with at least some of the replacement chips bearing the date code 9832. Between 2006 and 2008, KRANTZ sold and caused to be sold at least 900 chips with date code 9832 to Bay Components, the majority of which were sold to the Connecticut company. KRANTZ knew that the chips had originated from a parts supplier in China, and there was a high probability that the chips were falsely remarked not the original chips of the certain manufacturer as represented by the markings on the chip. He also avoided engaging in common practices in the industry, including those which Harry Krantz LLC routinely engaged in for other military parts, to avoid confirming that the chips were likely remarked. The investigation revealed that many of the chips were used in the assembly of U.S. Military and commercial helicopters.

So an unnamed Connecticut company purchased electronic parts from Bay Components, who in turn acquired them from Krantz. The unnamed Connecticut company rejected the first shipments, but permitted its supplier and lower-tier supplier to replace the rejected chips. Unfortunately, Krantz sourced the chips from China and knew they were likely to be counterfeit. The counterfeit chips were sold up the supply chain and installed on "U.S. Military and commercial helicopters." Now in fairness, let's note that this all took place a decade ago, well before the recent emphasis on counterfeit electronic part detection and prevention. So that unnamed Connecticut helicopter manufacturer really shouldn't be embarrassed that it failed to manage the situation. But still, there are some obvious lessons to be learned here.

First lesson: there aren't that many helicopter manufacturers in Connecticut. It's kind of obvious who the company is, and we expect Lockheed Martin will implement its own version of CEPDAS after the acquisition is finalized.

Second lesson: if your part supplier delivers a shipment of non-conforming parts, that's a *huge* red flag and should spark an immediate investigation. We're talking about QA folks para-dropping into the supplier's operation with no warning, along with sniffer dogs trained to

detect made-in-China chips. (Okay that may have been a bit over the top, but we suspect you get the drift.) Procurement should
not
treat that event as a business-as-usual supplier mistake, as it may well just be the tip of a nasty iceberg looming dead ahead. That kind of event is the announcement that the supplier's risk probability curve has reached an inflection point, and is quickly approaching a 100% certainty that your program is going to have significant negative cost and schedule variances. Does your supply chain team know what to do if there is such an event?

Third lesson: that unnamed Connecticut helicopter manufacturer may have an approved CEPDAS and, if so, its reaction and recovery costs may be allowable. But if not, then we bet a significant amount of unallowable costs were incurred. The negative impacts may be recoverable through litigation against the middleman supplier (Bay Components) or against Krantz directly. But that assumes that either or both companies have the financial resources to compensate the big unnamed Connecticut helicopter manufacturer. If the money (or insurance) isn't there, then we suspect the big prime may be SOL.

So here's a timely object lesson on the importance of securing your supply chain and implementing a strong CEPDAS. We've been ranting about this stuff for years, but we're not asking you to listen to us. We're asking you to look at the unnamed Connecticut helicopter manufacturer and learn from that company's misadventures.