Dromara Partners

Dilemma : 5 IT Provider business practices that can BACKFIRE in the U.S. Federal Market

SPECIAL REPORT

Abstract

This special report looks at five common business practices that technology providers are investing in to increase scale, grow top line revenue and drive cost efficiencies within their business model. Each is looked at in detail, providing both the value to the technology provider and the perception of these by U.S. Federal IT buyers. The report closes with our top three recommendations for technology providers to make sound business decisions and stay aligned with your U.S. Federal IT buyer community.

EXECUTIVE SUMMARY

The fundamental mission of a technology company is to create unique intellectual property that solves customer problems and quickly monetizes that asset to fuel growth for reinvestment in the business. Two common strategies implemented to achieve that mission are

Invest heavily in the single biggest market for your offering

Create or tailor your offering to address the unique needs of the marketplace for competitive advantage. With a projected $92 billion in FY19 Information Technology spend, you won't find a bigger opportunity than the U.S. Federal market.

Leverage a single offering to serve multiple markets

Reap value of one intellectual property source, accelerate revenue growth by selling the same offering without market customization and expand operational capability quickly.

However, when these strategies are embraced equally by technology providers, this common practice creates meaningful concern for U.S. Federal IT buyers who are continually pressed to meet evolving cyber-security obligations and are desperate to avoid being the agency whose name gets put into the press when a technology provider has a problem.

This special report looks at five common business practices that technology providers are investing in to increase scale, grow top line revenue and drive cost efficiencies within their business model. Each is looked at in detail, providing both the value to the technology provider and the perception of these practices by U.S. Federal IT buyers. The report closes with our top three recommendations for technology providers to make sound business decisions and stay aligned with your U.S. Federal IT buyer community.

THE FIVE INITIATIVES

The Five Initiatives are not stack-ranked by importance nor are they intended to represent the only business practices pursued in search of value.

They are simply the initiatives that we've worked most intimately with in our practice:

1. **Targeted Revenue Growth Initiatives in Foreign or Adjacent Markets**
2. **Distributed Global Product Development**
3. **Distributed Global Support Services**
4. **Optimizing the Global Supply Chain and Manufacturing Operations**
5. **IT System Consolidation**

1. TARGETED REVENUE GROWTH INITIATIVES IN FOREIGN OR ADJACENT MARKETS

Technology providers are fueled and their success is largely measured by revenue growth. To achieve growth, they have multiple levers to consider:

Taking more market share in existing markets	Growing market share in new or emerging markets	Developing or acquiring new offerings that allow them to compete in new markets	Expanding into adjacent markets via new partnerships, alliances or joint ventures

Deciding which or how to pursue these options is a careful balance and is usually determined by current success, financial strength, risk tolerance of the Senior Executive Team, macro level trends occurring in the market, and executive relationships with others in the industry.

Two scenarios that should resonate in terms of our Federal market discussion:

A concerted effort to grow revenue and share in a foreign market

A U.S. technology provider wants to grow their revenue outside of the United States as a strategic initiative and respond to Wall Street pressure. The data shows that the world's second largest IT market is China and they begin to invest in growth initiatives to break into this complicated market. They open up a Research Center in Beijing to better understand the needs of the market and engage with local partners and universities. They look to expand their product distribution with local partners and OEMs and investigate joint ventures with existing Chinese technology providers or ODMs (original design manufacturer) for local manufacturing capability. Logical and straightforward right?

An acquisition of a company or partnership to expand the market

A U.S. technology provider sees room for significant revenue growth and market expansion by acquiring or partnering with a known player in an adjacent IT market. After careful review of multiple global players, the company chooses a conservative path by forging a partnership with a firm based in the U.S. who has global reach. The partners announce a joint marketing/product integration campaign.

VALUE TO TECHNOLOGY PROVIDERS

In these scenarios, it appears to be all upside for our technology partner; both scenarios created an opportunity to address new markets and partners. They also leverage existing capabilities to achieve the revenue growth objective. To internal stakeholders of the technology firm this is a win; incremental revenue, modest expenditure, and no impact on current customers.

PERCEPTION OF THE FEDERAL IT BUYER

Make no mistake, U.S. technology providers who serve the Federal IT market are judged by the company they keep even if their business initiatives have no intended direct impact on their Federal customers.

In the first scenario above, this can be a big concern. The extent of that concern can range from multiple agencies seeking documented assurances detailing how knowledge of the technology they have deployed in their environments will be protected now that it is in the hands of a known threat to United States National Security to a full-on CFIUS (Committee on Foreign Investment in the United States) investigation if the company pursues establishing a joint venture with a Chinese company. Being judged by the company you keep is compounded by multiple recent disclosures of U.S. technology providers voluntarily sharing access to product source code to foreign entities for the purpose of inspecting for "backdoors."

In the second scenario above, what was not known to our technology provider was a team in Russia originally developed the foundation for the technology used by their new partner. Within the government, there are non-published "watch lists" of firms that the Intelligence Community closely monitors. In this simple use case, our technology partner unknowingly harmed their own brand within the Federal IT market despite efforts to grow revenue in non-Federal markets.

In both cases, we would expect the potential for revenue with current Federal clients to slow significantly. The challenge is you may not know you've gone into the "penalty box". You may also be challenged to know who within the agency you can have a timely and open dialog with in order to properly address all concerns.

2. DISTRIBUTED GLOBAL PRODUCT DEVELOPMENT

Quickly developing new product offerings is the lifeblood of a successful technology provider. Why would a company not want to tap into the intellectual horsepower and experiences of people that sit outside of the United States, take advantage of using all 24 hours each day to boost productivity, and leverage economic incentives provided by countries eager to attract foreign direct investment?

By leveraging pools of talent across the globe, companies are gaining access to:

Unique technical skills, access to new customer use cases and, in many instances, labor rates significantly lower than what can be found in U.S. markets.

New "local market" revenue pools as a result of direct investment, creation of new jobs, and relationships built within the local ecosystem.

Examples to consider:

ISRAEL
Known to produce leading experts in the fields of cyber-security and machine learning based upon the experiences and technologies readily deployed in the national defense of the country.

RUSSIA
Known for centuries for its prowess in science, research, and mathematics.

CHINA AND INDIA
Access to the world's deepest bench of engineering and mathematics talent, employees eager to make a difference, and attractive labor rates.

VALUE TO TECHNOLOGY PROVIDERS

For general managers of technology companies who are highly incented to create unique offerings, leverage the best talent, gain access to new markets, and manage costs to increase profitability, this is an incredible opportunity to leverage and almost impossible to ignore.

For local Sales Leadership in the new area of investment, there is a solid story to be shared with local government, customers, and partners defining how your company is investing hard dollars to show your commitment to the local market and they now have expertise they can leverage locally.

PERCEPTION OF THE FEDERAL IT BUYER

At its highest level, this is a National Security concern to a U.S. Federal buyer if a technology providers does not put in place and clearly articulate significant controls for employees or partners working on products sold to or deployed within a U.S. Federal site.

U.S. Federal agencies have always trusted that the final assembly of products is done and monitored by technology providers on U.S. soil to prevent malicious code or malware from being embedded in product. Additionally, within contract structures used to procure products, there are specific requirements to detail where these offerings are developed, manufactured, and supported.

For U.S. Federal agencies with a dependency upon a legacy product that may be deeply rooted into their operation, a change in the staff or location where updates are developed and source code repositories are maintained would be a major concern

3. DISTRIBUTED GLOBAL SUPPORT SERVICES

Providing a consistent and cost-effective support experience for all customers is a core objective for technology providers. To achieve that objective, support services have increasingly moved from someone who shows up to diagnose and repair a system at a customer site to layers of remote support staff and "self-healing" technologies that don't require a technology provider to pay for lots of staff being allocated to a small number of clients they can assist.

Examining the principal values of moving Product Development work to leverage global talent pools and experiences, we see similar trends for Support Services and some that are prioritizing technology over people:

The use of global call centers in The Philippines, India, Poland, and China continues to grow.

Increasing use of web-based technologies (Chat, Video) displaces or complements voice calls intended to remove complexity.

Increasing use of artificial intelligence, advanced analytics, and more integration with back end systems speeds the time to problem resolution.

Self-healing or self-reporting technologies continue to improve in order to avoid failures and reduce down time.

VALUE TO TECHNOLOGY PROVIDERS

For Senior Business Executives, achieving great customer service at the lowest cost is a key objective. Having any new capability that improves the consistency and quality of the customer experience, scales across multiple customers segments and allows for moving from fighting fires to knowing when to schedule maintenance activities is money well spent. In addition, if a provider can quantitatively get the same quality of U.S.-based service by using "off-shore" badged personnel or partners that offshoring adds to their bottom line or frees up investment dollars for required technology investments.

For local Sales Leadership in the new area of service investment, there is a similar story to be told to the government, local customers, and partners that your company is investing hard dollars to show your commitment to the local market and now there is expertise they can leverage locally. Furthermore with services, often times work is moved to large system integrators in a region, those firms can now also be consumers of the technology providers offerings.

PERCEPTION OF THE FEDERAL IT BUYER

U.S. Federal Agency relationships are historically built with local support staff that maintain the proper credentials and clearances. Given protection of government data and networks are a primary responsibility of all Federal IT buyers, introducing new technologies or processes that require connectivity is a non-starter.

Within procurement contract structures for products and support services, specific requirements for only U.S. Citizen on U.S. Soil service delivery are common. A technology provider must know the FAR, DFAR and any agency specific requirements and ensure these contract provisions are met

Access to site data by foreign nationals is a significant risk. Agencies will not allow assets to "report home" and also impose requirements to protect information that is contained within internal IT systems from being shared outside of the U.S. and only with those on a Need to Know basis

4. OPTIMIZING THE GLOBAL SUPPLY CHAIN AND MANUFACTURING OPERATIONS

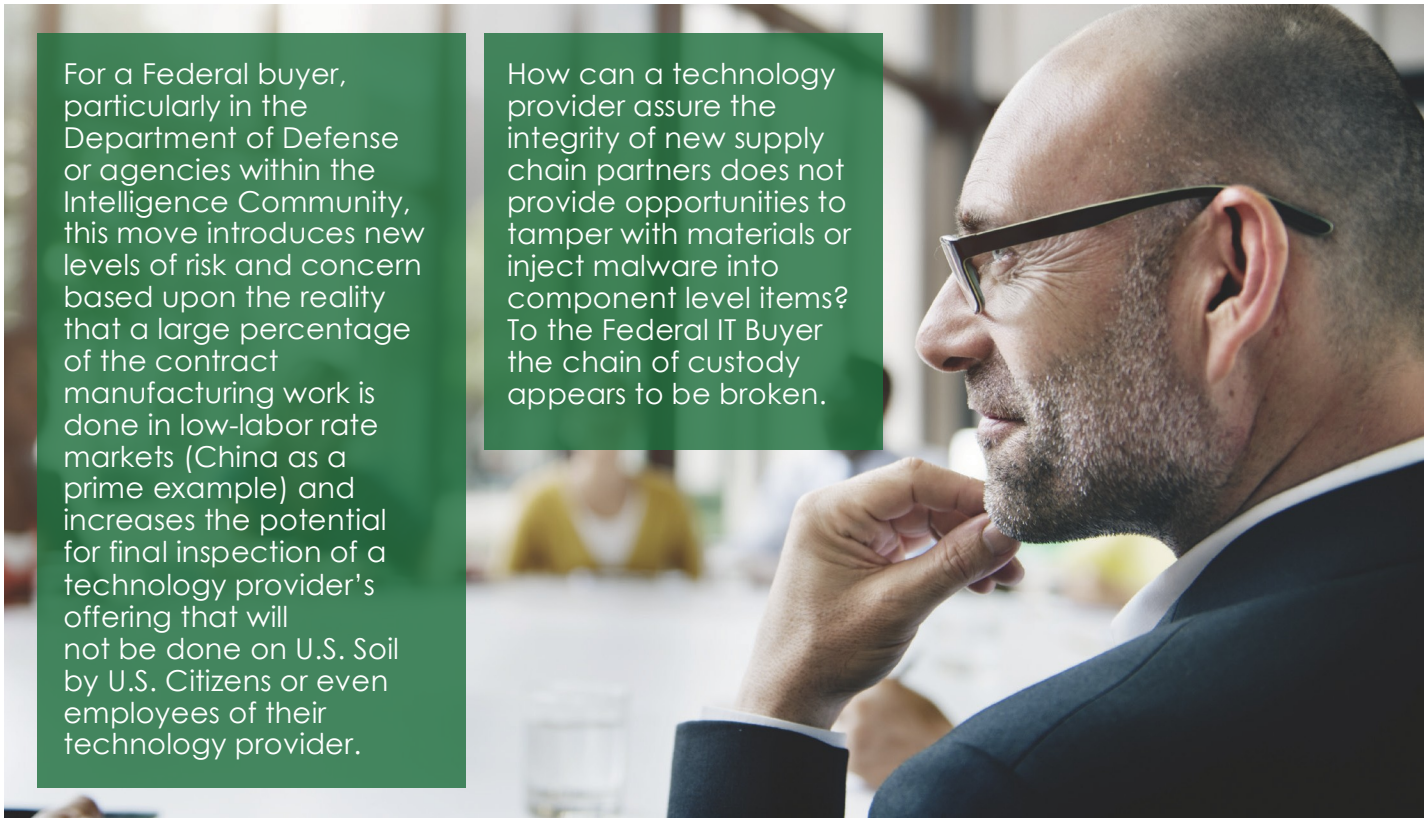
If a technology provider's growth rate is job number one, then creating a healthy and sustainable profit margin is job number two. A byproduct of that business reality is at some point in the lifecycle of every company there is inevitably a conversation within the C-Suite on "what is a core competency of this corporation that differentiates us in the market and what are we spending our cash flow on that can be better done by others?" In short, money is always needed to feed new revenue growth and intellectual property development for the technology provider to be a viable enterprise for years and decades to come.

A well-tuned supply chain and predictable manufacturing capabilities are critical pillars for any technology provider to build upon. How can you deliver your value and outstanding support to your customers if you don't intimately know the individual components and control the capability to assemble them into a finished good? It turns out that in 2018, it is a lot easier to achieve that mission using third-party expertise than in prior decades. The trend to use "COTS" (commercial off the shelf) components coupled with a wide range of large and competent contract manufacturers has allowed companies like Apple and Cisco to scale with incredible ease and profitability.

VALUE TO TECHNOLOGY PROVIDERS

The ability to leverage contract manufacturing capabilities to produce the same or incremental product offerings without having to use precious capital on building/maintaining/staffing component or final assembly manufacturing operations. There also can be significant supply chain cost advantages if you can leverage the power of your contract manufacturers in new buying arrangements. This can be done through unique purchasing contracts or simply leveraging the scale of buying common components for multiple customers

PERCEPTION OF THE FEDERAL IT BUYER



Further defining the serious nature of this issue, today there can be specific clauses embedded within agency procurement contracts that explicitly prohibit the drop-shipment of any product to them from a contract manufacturer and define specifications on conditions of components used in the product.

5. IT SYSTEM CONSOLIDATION

Like many things in business, the more similar "things" that you operate and have to provide ongoing care for, the harder your job becomes. Additionally, as they grow, the more time, people and money you have to dedicate to keep them all current. The job of a CIO at a technology provider is becoming increasingly complicated as they are tasked with:

Delivering a stable application and operating platform the entire business depends on to function on a 24x7x365 basis.	Delivering new technology capabilities that enhance the business's ability to generate new revenue and keep clients happy.	Maintaining the required controls to guarantee compliance with a growing list of global regulations.

A common practice to achieve these difficult tasks is to consolidate items put in place to meet specific functional requirements into broader enterprise capabilities or to take multiple systems that perform the same function into a single instance.

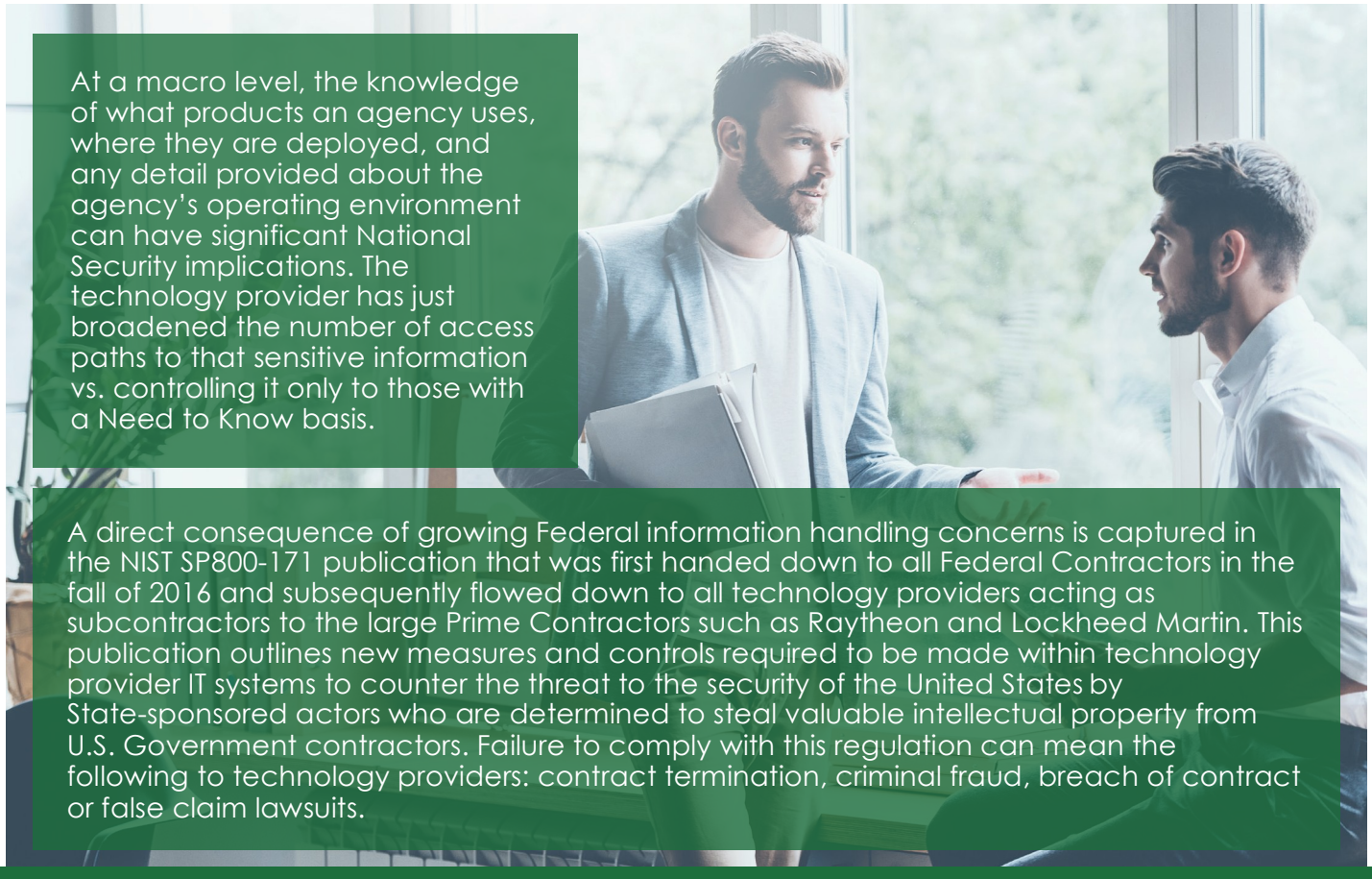
For illustration purposes only, within a technology provider, there are likely multiple systems of record (databases) for how different parts of a company engage with customers and prospects. A sales database, a marketing database, an electronic licensing database, and a customer support entitlement database – you get the picture.

A logical move would be to stop managing all of these items individually and pool them into a single resource that can be leveraged by multiple functions. Take this example and play it out against other systems and applications and you can see why this is a high-value initiative!

VALUE TO TECHNOLOGY PROVIDERS

The IT team gains new levels of control and consistency across the same dataset. They create a cost synergy opportunity to eliminate the amount of time people spend on the care and feeding of all of the individual items. The real savings generated can either be "returned" to the business for revenue/IP growth initiatives or invested within the IT domain to deliver new capabilities bucket.

PERCEPTION OF THE FEDERAL IT BUYER



At a macro level, the knowledge of what products an agency uses, where they are deployed, and any detail provided about the agency's operating environment can have significant National Security implications. The technology provider has just broadened the number of access paths to that sensitive information vs. controlling it only to those with a Need to Know basis.

A direct consequence of growing Federal information handling concerns is captured in the NIST SP800-171 publication that was first handed down to all Federal Contractors in the fall of 2016 and subsequently flowed down to all technology providers acting as subcontractors to the large Prime Contractors such as Raytheon and Lockheed Martin. This publication outlines new measures and controls required to be made within technology provider IT systems to counter the threat to the security of the United States by State-sponsored actors who are determined to steal valuable intellectual property from U.S. Government contractors. Failure to comply with this regulation can mean the following to technology providers: contract termination, criminal fraud, breach of contract or false claim lawsuits.

TOP THREE RECOMMENDATIONS FOR TECHNOLOGY PROVIDERS

What is a technology provider to do in order to successfully grow their business and keep their Federal IT buyer community aligned?

1 Appoint a C-Suite owner to ensure you are having the right internal conversations before you cause a disruption in this critical market. National Security and Federal Advocacy need not be that person's full time job but without an Executive Sponsor to champion healthy cross functional dialog and respectfully challenge the status quo, the daily rhythm of your business will create events that will put you at high risk. The type of risk that takes significant time, effort and dollars to mitigate

2 Own your future success by diligent tracking and scenario building to determine how a change in a broad-based regulation (e.g., NIST SP800-171) or contract level changes at an Individual agency impact your current business operations. Know where the sources of those prospective changes will come from and build an open communication path for employees or partners to bring forth ANY potential requirement change. Hold one person in your company accountable to owning this process and needed outcomes; otherwise, you quickly create an environment where functional teams, without malice intended, will choose what may be best/cheapest/easiest for them versus a solution for the entire company.

3 Be proactive in building, fostering and going out of your way to communicate directly with your U.S. Federal clients, contracting executives and agency leadership and Prime Contractor Partners before making major market moves. Not an easy task but, if they understand the context of your planned action, the boundaries you have put in place to protect their interests and that you care enough to get their input before you make a move, your credibility will grow and the scope of their concern reduces dramatically. (Side Note: It will be very interesting to understand the long-term consequences of Intel's decision, as reported by the Wall Street Journal, to pre-brief their Chinese partners of the Spectre and Meltdown flaws while allowing the U.S. Government to get the news via regular public disclosures.)

CONCLUSION

The U.S. Federal IT market provides for outstanding revenue opportunities for all technology providers to grow their business. The best of the best understand that this is a rapidly changing landscape that requires precision. These top technology providers include a U.S. Federal voice into all of their strategic planning efforts and, at their core, know the compelling revenue opportunity of the Federal IT market is matched with an extensive "body of obligations" that requires daily care and feeding. To succeed in this market, an unwavering commitment to maintaining a strong knowledge base of current U.S. Federal requirements, a tight alignment of selling and delivery efforts, trusted U.S. Federal customer relationships and strong C-Suite engagement are all critical.

Dromara Partners

www.dromarapartners.com

info@dromarapartners.com
+1 508-205-9775