From Service to Product:

An Assessment of the Washington, DC Metro Region's Cybersecurity Industry

April 6, 2017

A collaboration between

AMPLIFIER ADVISORS

Jonathan Aberman, Managing Director
Michael Hoffman, Executive Editor
Jeffrey Blair, Research Director

KOGOD SCHOOL of BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC

The Initiative for Business in the Capital

Erran Carmel, Professor & Director
Drew Bailey, Research Assistant
Sam Woods, Research Assistant
Rhys Leahy, Research Assistant

Table of Contents

Executive Summary 1

Introduction 2

- Background for this Report 2
- What Do We Mean by "Cybersecurity Industry"? 3
- What's the Difference Between a Product and Service Business? Why Does it Matter? 3

Report Findings 5

- Methodology and data sources 5
- Company categorization/ coding 5
- Client Focus Analysis 5
- Product-Solution Analysis 6
- Crossing Client Focus & Business Focus 7
- Location Analysis 10
- Small Business Status (sample only) 12

Conclusions and Recommendations 13

- Conclusions 13
- Recommendations 14

EXECUTIVE SUMMARY

The cybersecurity industry in the Washington, DC metro region ("the Region") is well established. This report lays out its size, its activities, and a path for future development.

This report identifies 858 cybersecurity businesses in the Region.[1] The Region's cybersecurity firms showed a high concentration of service and solution-based business models. Only 5% of them are focused on developing cybersecurity products. This profound lack of product-based cybersecurity industry activity is striking, especially in light of significant regional investment in software product startup accelerators and incubators.

Cybersecurity businesses are unevenly distributed across the Region. Two-thirds of the companies are in Northern Virginia, with the remainder in Maryland and Washington, DC. More than half of all companies are in two counties – Fairfax County, Virginia, and Montgomery County, Maryland. In fact, 306 cybersecurity firms call Fairfax County home versus 45 in Washington, DC.

The cybersecurity industry skews heavily towards the federal government as a source of revenue. Only 6% of the firms identified in this report worked with clients exclusively in the commercial sector. Meanwhile, one out of three cybersecurity companies in the Washington, DC metro region worked exclusively in the government sector.

The independent work undertaken by the Kogod School of Business' Initiative on Business in the Capital (the "Kogod Team") incorporated into this report validates and reinforces prior work publicly disclosed by Amplifier Advisors. The Region faces not only the possibility of significant changes in federal spending, but also the continued progress of competing regions in the United States in developing market leading software product companies.

Accordingly, there is an urgent need for the Region to understand that while it currently has a strong cybersecurity industry, the industry is fragile and the Region is not well-positioned to be a leader in the future. Effective efforts must be undertaken to lessen the region's reliance on federal revenue and to increase the number of commercially focused, product-based cybersecurity businesses.

[1] The Washington DC, metro region encompasses the District of Columbia, five Maryland counties (Montgomery, Howard , Prince George's , Anne Arundel and Charles) and four Northern Virginia counties (Arlington, Fairfax, Prince William and Loudoun).

INTRODUCTION

BACKGROUND FOR THIS REPORT

Over the years, the Region's policy and business discussions have repeatedly considered making cybersecurity the focal point of economic development. The general consensus that the Region is already strong in this industry and that it has significant potential for additional business creation and job growth is supported by a number of independent sources. The Cybersecurity 500 list places the Washington, DC metro area just behind Silicon Valley.[2]

However, there was little publicly available information on the composition and activities of the local industry. Over the last 12 months, Amplifier Advisors, the manager of the Tandem Innovation Alliance and its affiliate Tandem National Security Innovations ("TandemNSI"), has undertaken several projects to collect the data and to evaluate this economic opportunity. Two results of this work are the *TandemNSI Cybersecurity Industry List* and a report, *Building Entrepreneurial Innovation in the Greater Washington Region* (the "2030 Group Report"). Additionally, Amplifier Advisors has undertaken several nonpublic projects that further inform its data gathering and analysis.

Amplifier Advisors believes that previously disclosed data paint a picture of a regional cybersecurity industry with the following key attributes:

- Many privately-held cybersecurity businesses are headquartered in the region.
- There is an uneven distribution of these businesses within the Region.
- These businesses derive collectively a high percentage of their business revenues from federal spending.
- Most of these businesses deliver service and solutions, notwithstanding a high level of regional investment in software product business incubators and accelerators.

If, in fact, these conclusions are correct, the Washington, DC metro region faces significant challenges if it is to develop its cybersecurity industry and compete with other U.S. regions with proven expertise in developing commercially focused cybersecurity product businesses.

Amplifier Advisors asked the Kogod School of Business' Initiative for Business in the Capital to review the data collected and provide an independent assessment. This report provides

[2] The Cybersecurity 500, by region: http://cybersecurityventures.com/cybersecurity-500/ 117 Silicon Valley based companies; followed by 54 companies in the DC metro area,

the result of the Kogod Team's analysis and its conclusions. As will be described below, the independent review and analysis further reinforces and confirms Amplifier Advisors' prior work.

What Do We Mean by "Cybersecurity Industry"?

The cybersecurity industry comprises the business and individuals that provide cybersecurity products, services or solutions. It is a large market opportunity – estimated to be as much as $77 billion worldwide.[3] The United States federal government is a large portion of this market -- $19 billion or more will be spent in 2017 by some estimates.

Cybersecurity employs a broad range of technologies, including computer hardware (and related internet-connected appliances such as routers and physical devices that provide monitoring), sensors, data sciences and analysis, machine learning and artificial intelligence. And as protecting data and infrastructure becomes more difficult at the same time that society and business increasingly demand greater data integrity, the need for cybersecurity appears to be insatiable.

What's the Difference Between a Product and Service Business? Why Does it Matter?

Businesses provide a service, a product, or a combination -- a solution. Service businesses can be innovative and unique, but their ability to scale up and grow rapidly is limited by how quickly they can hire and train new people. A business with an innovative product, on the other hand, is able to scale because production capacity can generally be added quickly. Intellectual property rights protecting products and processes – particularly patents and trade secrets – can form a high barrier to entry by competitors.

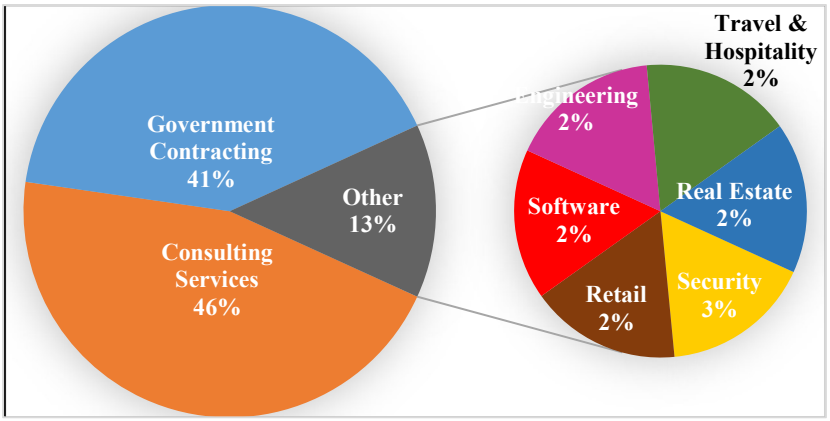
A solution-based business's growth potential lies somewhere between that of product businesses and service businesses because the need for trained service providers can be a drag on the product portion of the business. How much of a drag depends on the relative proportions of service and product that go into the solution. It can be difficult to coordinate the growth of the two components. Of the three types of innovation-based businesses, product companies tend to grow fastest.

For purposes of illustration, the Region's most rapidly growing companies continue have the federal government as a primary customer. Moreover, these businesses tend to be consulting or service-based businesses, rather than product-based. Between 2015 and 2016, the percentage

[3] *The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment and Industry Statistics*, Forbes Magazine October 16, 2015.

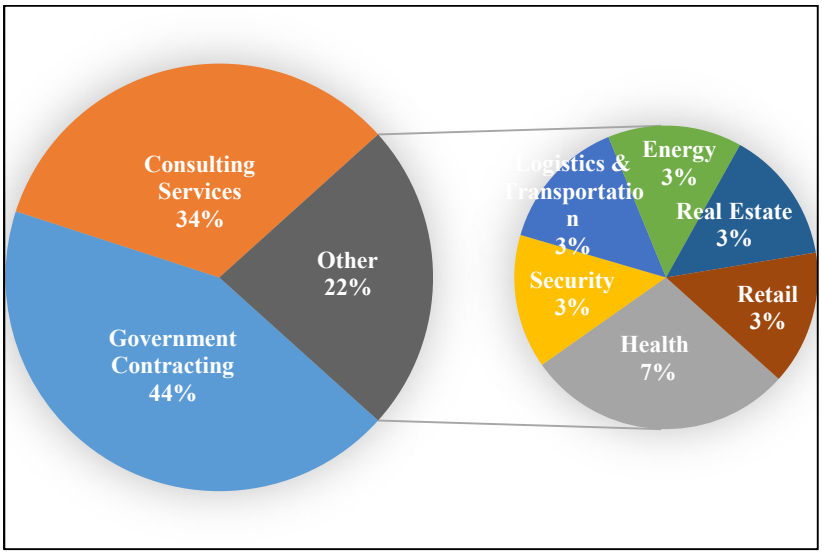
of consulting businesses dramatically increased, while the overall percentage of product-based businesses remained constant.

Exhibit 1: Composition of the Greater Washington Region's Fastest Growing Companies, 2016



Source: Inc. 500

Exhibit 2: Composition of the Greater Washington Region's Fastest Growing Companies, 2015



Source: Inc. 500

REPORT FINDINGS

METHODOLOGY AND DATA SOURCES

This report is primarily based upon data found on firms' public websites. It expands upon the TandemNSI Cybersecurity Industry List. In preparing the list, Amplifier Advisors had reviewed publicly available business listings and private lists developed by leading community organizations and jurisdictions, conducted interviews with market participants and analyzed federal spending on cybersecurity products, services and solutions. The TandemNSI Cybersecurity Industry List identified 972 Maryland, Virginia, and Washington, DC cybersecurity firms. The TandemNSI Cybersecurity Industry List included companies for the entire states of Maryland, Virginia and Washington, DC. The Kogod Team limited its review to businesses in the Washington, DC metro region.

The Kogod Team identified a small number of miscounted businesses in its review, but validated nearly all of the businesses listed on the TandemNSI Cybersecurity Industry List that were located in the Washington, DC metro region. Its final list included 858 of the 972 firms identified by TandemNSI. This targeted list of 858 firms became the basis for the Kogod Team's subsequent data analysis.

COMPANY CATEGORIZATION/ CODING

The Kogod Team made the following categorizations to parse the businesses on its cybersecurity industry list:

- Client sector variable data was coded "commercial," "government," "both," or "not enough information" based on firm self-identified client sector information. Any federal, state, or local government clients were considered to be part of the government sector.
- The location variable data was coded by county/city based on the firm location.
- On a sample basis, the Kogod Team also coded small business status "yes" or "no," based on firm website self-identification.

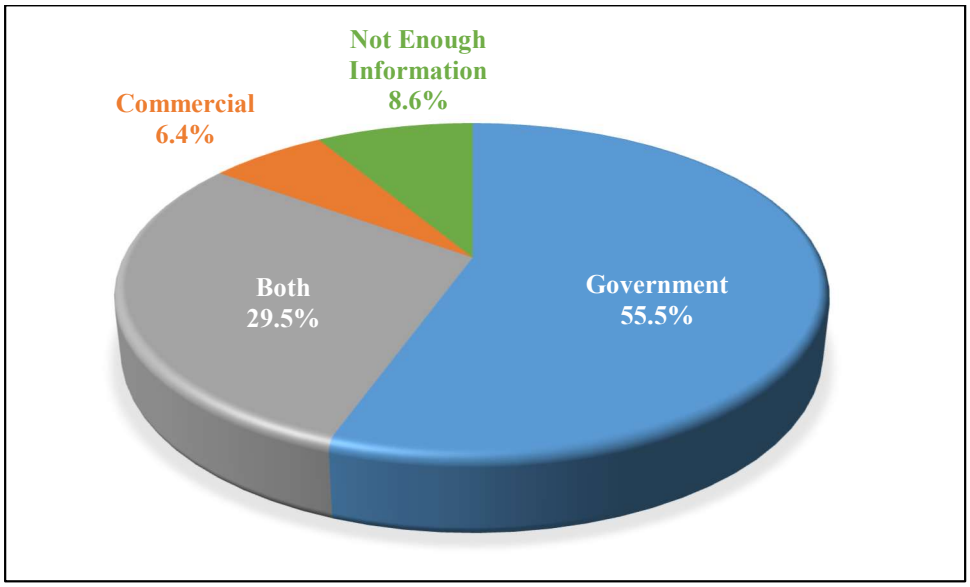
CLIENT FOCUS ANALYSIS

The Kogod Team identified a high proportion of cybersecurity firms focused partially, or solely, on the government sector. Of the 858 firms based in the Region, 29.5% reported working exclusively with the government sector. Additionally, 55% of the sampled firms reported

working with both government and commercial clients. Only 6% of firms reported working with commercial clients exclusively. The client mix of the remainder could not be identified.

This composition is consistent with the TandemNSI Cybersecurity Industry List and underlines a significant reliance on the federal government as a customer for the region's cybersecurity businesses. The Kogod Team cautions that for the 55% of companies it identified as doing both commercial and government work, the proportion of business in each sector cannot be determined without disclosure by the firms themselves. Therefore, the magnitude of risk to the Region's cybersecurity industry from material changes in federal spending cannot be completely assessed. It is abundantly clear, however, that the region's ability to withstand significant changes in federal spending will be found in the firms that have a balanced client mix.

Exhibit 3: Firms by Client Focus



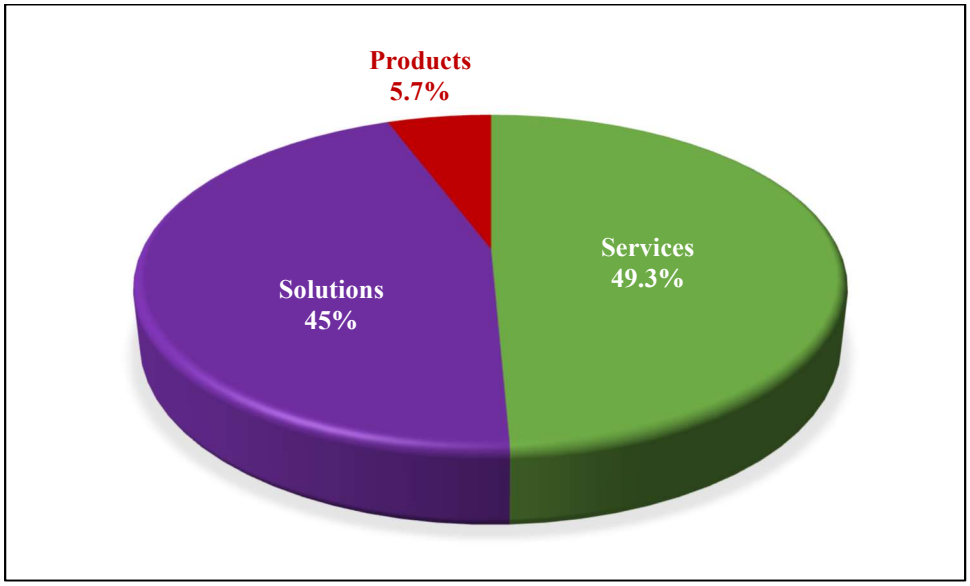
PRODUCT-SOLUTION ANALYSIS

Along with the heavy reliance on government spending, the Washington, DC metro region's cybersecurity industry features a high proportion of cybersecurity firms providing services or solutions, and relatively few firms focused on developing products. Of the 858 firms identified by the Kogod Team, only 5.7% reported selling products.[4] By contrast, 94.3% of the sampled firms reported providing services or solutions to government and commercial clients. This data is consistent with the TandemNSI Cybersecurity Industry List.

[4] Note that this is higher than the 4% found in the TandemNSI List because of the tightening of the base company dataset.

- **Products**. The company primarily produces cybersecurity products.
- **Services**. The company primarily provides cybersecurity services.
- **Solutions**. The company provides cybersecurity services, but also sells products. These could be resellers operating as consultants or product manufacturers who also provide support and analytics with their products.

Exhibit 4: Firms by Business focus



CROSSING CLIENT FOCUS & BUSINESS FOCUS

The Kogod Team examined the intersection of client focus (government versus commercial) with business focus (product/service/solution). The results are in Table 1. It is clear from these results that the vast majority of the Region's firms are in the (yellow) shaded areas at the intersection of companies that serve government or government and commercial clients with services and solutions. There are 699 firms in this grouping, representing 81% of total firms. (In fact, the percent of firms in this grouping is likely higher because some firms in the "other" category would probably be classified here).

The Kogod Team took a sample of these firms and constructed archetypes of each of the four groupings as shown in Table 2. This micro-segmentation highlights that the Region's cybersecurity firms are focused on the federal government, and many have no presence outside the region. It appears that many of these firms focus on national security for at least some of their federal revenue.

Table 1: Cross-tabulation of Client Focus by Business Focus

	Commercial	Government	Both	No Data	Total
Products	6	3	15	5	**29**
Services	19	**152**	**228**	25	**424**
Solutions	31	**99**	**220**	36	**386**
Other	0	2	11	6	**19**
Total	**56**	**256**	**474**	**72**	**858**

In Percentage

	Commercial	Government	Both	No Data	Total
Products	11%	1%	3%	7%	**3%**
Services	34%	**59%**	**48%**	35%	**49%**
Solutions	55%	**39%**	**46%**	50%	**45%**
Other	0%	1%	2%	8%	**2%**
Total	**7%**	**30%**	**55%**	**8%**	

Table 2: Archetype of 699 Firms in the 4 Main Regional Grouping Types

	Government & Commercial Services	Government & Commercial Solutions	Government Services	Government Solutions
Founded	Founded between 2002 and 2007		Established in the last ten years	Founded between 2008 and 2013
HQ	HQ in WDCMA but has other locations			No locations outside of DC area
Size	Typically employs 12 to 50 employees	Range from 8(a) small business, to boutique firms, to multinational corporations	Often 8(a) Small Business and subcontracts with larger firm, such as HP, Northrop Grumman, or BAE Systems	Tends to be small (as measured by contract vehicle)
Clients	Fortune 500 companies and national security.	Range of business and government clients but tends to be national security focused	Government work with at least one national security organization and often works exclusively with national security	Sells to a diverse set of agencies
Specialty	General IT services, network security services, product evaluation, and assistance with meeting government compliance standards		Services such as threat defense, vulnerability assessments, and security audits or specific IT services such as network engineering and design or cloud computing and storage management	Program management, cybersecurity solutions, or software engineering services

LOCATION ANALYSIS

The Kogod Team identified the geographic distribution of cybersecurity firms operating in the Region. It determined that 62% of the firms are located in Virginia, 33% in Maryland, and 5% in the District of Columbia. This distribution shows that while the District is the geographical epicenter of the region, almost the entire industry is based outside the District.

When segmented by county/city**,** 53% of the firms were located in just two counties: Fairfax County, Virginia, and Montgomery County, Maryland. Including the firms located in the independent City of Fairfax, the combined share of these areas jumps to 58% of all regional firms. The majority of counties/cities held between 30 and 70 firms: Arlington County (65), Howard County (53), District of Columbia (45), Loudoun County (45), the City of Alexandria (40), Anne Arundel County (39), and Prince George's County (32). Two counties and three independent municipalities had fewer than 20 firms: Falls Church (17), Prince William County (15), Charles County (5), Manassas (5), and Manassas Park (1).

This geographic distribution is also consistent with the 2016 TandemNSI Cybersecurity Industry List.

Exhibit 5: Cybersecurity Firms by County/City Location

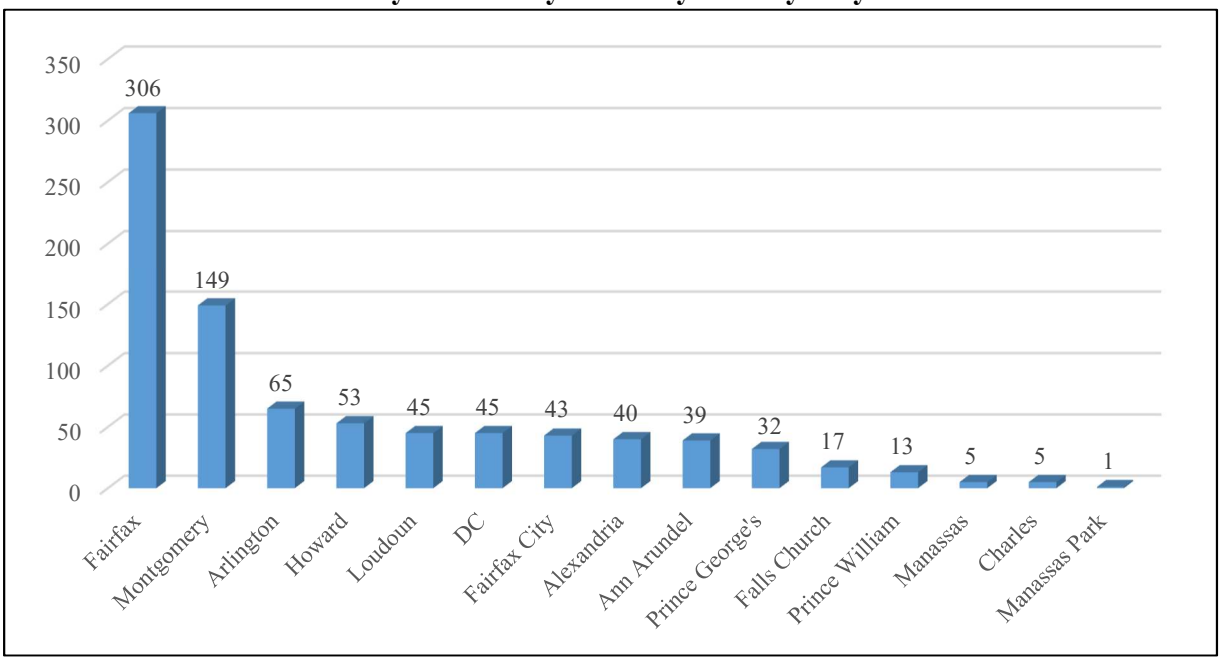


Exhibit 4: Cybersecurity Firms by State

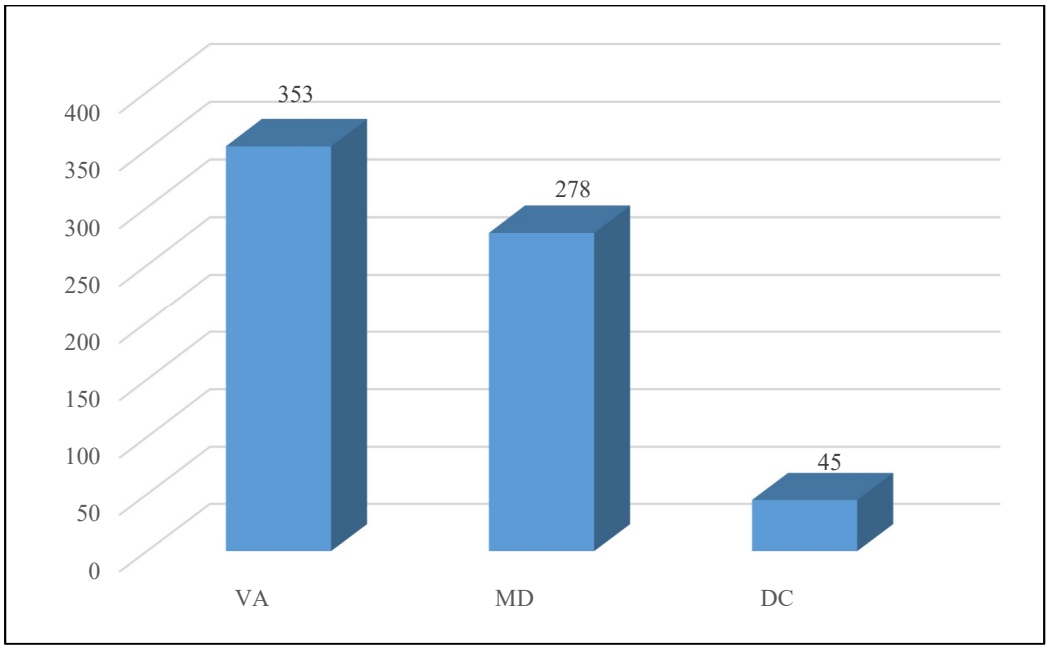
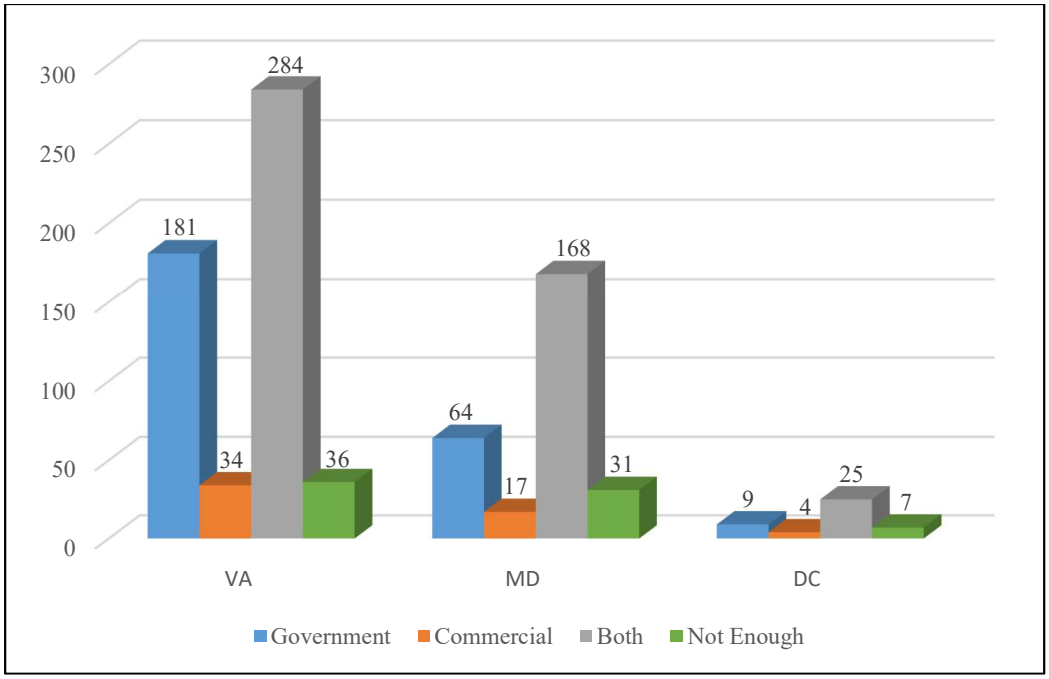


Exhibit 5: Firms by Client Sector Segmented by State

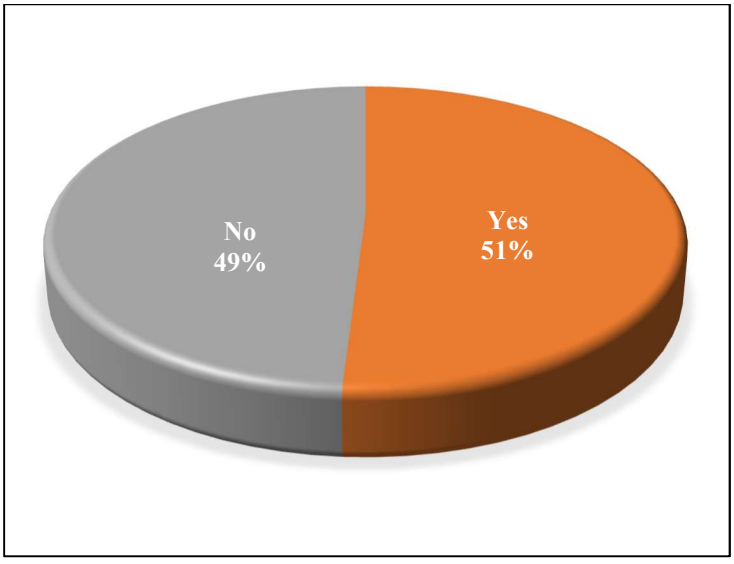


SMALL BUSINESS STATUS (SAMPLE ONLY)

While the focus of this report is on the clients and types of businesses, the Kogod Team also wanted to look at the relative size of cybersecurity firms in the region. It analyzed a random sample of 100 firms. It then determined whether the firms self-identified as a "small business" under applicable federal regulation, stating, for example, "we are a veteran-owned small business" or certifying eligibility for certain federal contract vehicles reserved for small business. The Kogod Team determined that 51% of the sample size described themselves as small business for the purposes of obtaining federal contracts.

The remaining 49% did not self-identify as small businesses. The Kogod Team could not determine whether this is because they are not small businesses or because they do not believe that this description is helpful. However, we found this concentration still illustrative of the potential fragility of the Washington, DC metro region's cybersecurity industry. If so, many businesses rely on marketing themselves as eligible contracting partners for federal contract set asides and preference programs. This suggests a reliance on the government as a customer that is particularly subject to changes in federal spending, something that is particularly concerning since -- by their nature -- small businesses are unlikely to have diverse customer bases and revenue.

Exhibit 6: Firms by Small Business Identification



*sample of 100 total firms

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS

The Washington, DC metro region has a vibrant cybersecurity industry. It has a high concentration of demonstrable entrepreneurial talent and human capital devoted to this industry. Those who point to the region as being a leading location for cybersecurity businesses now have solid data to support this statement.

However, the hard data in this report (and the original Amplifier reports) enables us to see more clearly the composition of the industry. It is dangerously reliant on the federal government as a source of business revenue. It is also clear that the region's cybersecurity businesses are clustered in service and solution business models, at the same time that the better growth opportunities are found in product-based businesses.

This creates two large challenges if the Region is to maintain its position in the cybersecurity industry. First, to the extent that commercial customers desire the delivery of product-based innovations, or to the extent that the rapid growth potential of product-based businesses is desirable, the Region has considerable work to do to configure itself to produce these types of businesses. Notwithstanding considerable regional investment in accelerators and incubators, there is a large gap between programmatic intention and demonstrable success.

Second, there is a marked reliance on the federal government as a source of revenue. Although the allocation between government and commercial revenues is not easily determined without individual company disclosure, the data show that many companies are reliant exclusively on government purchasing. And it can be hypothesized that a significant portion of the remaining businesses not identified in this study would suffer materially adverse harm were it to lose government derived revenue.

The regional industry has failed to grow a more balanced portfolio that is more product-focused and commercial-focused. This leaves the Region exposed to changes in federal expenditures.

RECOMMENDATIONS

We believe that to progress and further understand the composition of the cybersecurity industry in the Washington, DC region and to provide for its continued growth, a number of specific actions should be undertaken:

- **Company revenue analysis.** An assessment on a per company basis of the allocation of commercial to government sales should be undertaken to assess the region's actual reliance on federal spending for cybersecurity.
- **Industrial support organizations.** New resources are needed to support businesses in order to identify commercial customers. Most of the regional firms have little to no experience in selling to commercial customers. A vertically integrated business consortium that combined larger commercial buyers with small business vendors is highly recommended.
- **Business training.** Approaches to building product-based cybersecurity businesses must be expanded to include not just business formation, but also business expansion or business change. The large number of service and solution-based businesses demonstrate a strong need for training in product development and commercialization.
- **Federal funding for innovation.** Regional political leaders must act to ensure that federal government cybersecurity outreach and innovation spending continues to include the Washington, DC metro region.