MONTGOMERY COUNTY ECONOMIC DEVELOPMENT CORPORATION

2017

GROWING THE CYBERSECURITY INDUSTRY IN MONTGOMERY COUNTY

Growing the Cybersecurity Industry in Montgomery County
March 7, 2017

OVERVIEW

In the summer of 2016, the board of the Montgomery County Economic Development Corporation ("MCEDC") identified cybersecurity as a target industry, and commissioned a report by Amplifier Advisors entitled "Building a Cybersecurity Industry in Montgomery County." The Amplifier report was submitted to the MCEDC board in September 2016.

In November 2016, a group of local cybersecurity CEOs and experts was convened by MCEDC and tasked with vetting the Amplifier report and then recommending strategic initiatives that would put Montgomery County, MD "on the map" as a world-renowned cybersecurity ecosystem.

The workgroup was comprised of:

Nigel Jones, CEO Koolspan (Workgroup chair)

John Abeles, CEO System 1, Inc.

Brian Chambers, CIO EagleBank

Mark Firley, Computer Security Analyst, IBM

Chris Ghion, CIO Adventist Healthcare

Ajay Gupta, CEO Health Solutions Research Inc.

Susan Prince, National Cybersecurity Center of Excellence

Ola Sage, CEO CyberRX and CEO e-Management

Tien Wong, CEO Lore Systems

The workgroup met three times. The first meeting included a presentation by Amplifier Advisors, about the regional cybersecurity industry, including current strengths and weaknesses. The second meeting included Jason Stead, a cybersecurity purchaser at Choice Hotels, and Todd Simpson, CIO at FDA. Those experts, along with workgroup members Chris Ghion and Brian Chambers, provided insight regarding the cybersecurity needs of big buyers and anchor institutions (non-profits), as well as their technology evaluation and purchasing processes. During the workgroup's final meeting, it unanimously agreed to five recommendations.

The workgroup is pleased to offer the MCEDC board a holistic approach to supporting the emerging cybersecurity industry. The recommendations are based on the original Amplifier report, with some modifications informed by the group's collective experiences working in the industry. Each of the five priorities in this memo are structured similarly: there is a Model Programs section, which includes relevant initiatives to consider; a Project Cost section; a set of Implementation Steps; and a list of potential Partners.

The workgroup understands that these recommendations are substantial. In addition to the considerable financial investments required to execute these tasks, their implementation will also demand focus and tenacity from MCEDC's board and business leaders. The workgroup asks MCEDC to dedicate the staff and resources necessary to implement these priorities, beginning this fiscal year. In return, several members of the workgroup will continue to participate in an advisory capacity, if requested by MCEDC. Value will certainly come to cybersecurity businesses through the implementation of any combination of the recommendations – it's not all or nothing. Having said that, when implemented together, these recommendations will have an even greater chance of transforming the emerging cybersecurity industry.

1 **Create a consulting team of cybersecurity experts who can assist companies in evaluating and purchasing new, local cybersecurity technologies.**

Companies and anchor institutions that buy local products are essential to a healthy, sustainable economy. The workgroup wants to ensure that Montgomery County's cybersecurity businesses can grow to meet the demands within our regional economic ecosystem. To learn more about the opportunities available for locally developed cyber products and services, the workgroup invited CIOs from a local health system, bank, hotel and a federal installation to share their cybersecurity needs and procurement practices.

Not surprisingly, the threshold question for CIOs, regardless of their industry, was "does the product/service work?" Additionally, the CIOs explained the importance of long-term relationships with their contractors as well as some of their goals related to minority procurement.

Based on feedback from the CIO panel, the workgroup recommends that MCEDC create some type of expert-led evaluation group, like the federal 18F program listed below, or, at a minimum, explore a third-party certification of cybersecurity products/solutions/services, which will facilitate the purchase of local products by area institutions and companies.

MODEL PROGRAMS:

18F

The Amplifier report suggests the federal 18F program as a model consultative group, which applies emerging technologies to government problems.

The origins of 18F can be traced to 2012, when President Obama initiated the Digital Government Strategy. Through the evolution of policies and refinements, the "18F" project was formally announced in March 2014. Housed within the General Services Administration, 18F's purpose was to "make the government's digital services simple, effective, and easier to use for the American people." This included software and website development for government agencies. By March 2016, 18F offered five types of services to the government:

- Customer Partner Solutions: Providing federal agencies with specific IT solutions
- Products and Platforms: Developing products and platforms to be used government-wide
- Digital Acquisition Services and Marketplaces: Writing agency RFPs assisting IT purchasing
- Transformation Services: Working with agencies to increase digital capacity and modernization
- Learn: Providing agencies with best practices, workshops, reference guides

18F's administrative process includes entering into service agreements with client agencies and then collecting payment from those agencies. 18F has come under scrutiny for a several reasons, the latest highlighted in the October 2016 report by the Office of Inspector General (OIG), which noted 18F's net operating loss of $36M by the end of FY16.

The administrative set-up and poor fee-collection track record of 18F is, in many ways, immaterial to MCEDC, but the takeaways of the OIG report are: 1) it's easy to underestimate the amount of resources it takes to evaluate, recommend and procure the proper technologies when serving a wide variety of clients; and 2) we should be mindful about hiring experts/staff too quickly, without a revenue stream capable of supporting the expense.

Gartner/Savenia Labs

There are two, private-sector examples that provide third-party product evaluation/testing:

Gartner is a large, nearly 40-year old research and advisory firm that provides clients with analyses, evaluation and recommendations for their technology needs. Through its research methodology, Gartner provides insight on the competitiveness of technologies and can recommend outstanding vendors. The upside of a company/vendor receiving a positive Gartner evaluation is Gartner's solid reputation, which is backed by several thousand employees that have the resources to rigorously review products/services. The downside is that unless a Gartner analyst provides a vendor with the opportunity to present a briefing on its product, a vendor may never become part of a recommendation. Some local companies have expressed that Gartner briefing process is cost/time prohibitive.

On the other end of the private-sector spectrum is Savenia Labs, a small Bethesda-based business founded in 2009 by John Jabara. Savenia Labs is an independent testing laboratory and information services company that provides energy and environmental impact ratings on popular appliances, electrical products and homes. The Savenia Labs rating system is growing in national recognition, and is used by consumers to assist them in their purchases of products. Though not a cybersecurity company, Savenia shows that a local need for third-party verification can be met with a local entrepreneurial solution.

County Pilots

While MCEDC determines the cost/benefit of creating an expert evaluation team, MCEDC should work with the County Executive to provide more opportunities to deploy new cybersecurity technology within county government. Successful deployment of local products can serve as important traction for local companies seeking additional capital and the county can be an important reference for small cyber companies selling to commercial buyers.

IMPLEMENTATION STEPS:

In the next 90 days, MCEDC should determine:

- The level of demand from regional buyers willing to pay for an expert vetting/evaluation process of local technology;
- The willingness of regional buyers to rely on Gartner's (or another entity's) validation of local technology;
- The level of demand from local cybersecurity suppliers who want to be evaluated, and would they be willing to pay for that service; and
- How to engage the private sector in meeting this need.

PROJECT COST:

The Amplifier report estimates $100K-$1M to implement an expert consulting team, although the cybersecurity workgroup is unclear about the financial impacts until MCEDC agrees to a model.

If the solution is creating an expert panel, then professionals will need to be paid, along with local students and staff from USG and Montgomery College to assist with the consulting team's work.

If MCEDC just subsidizes small companies' participation in the Gartner process, or releases an RFP to allow the private sector to fill the void in evaluating local technology, then the costs will vary.

PARTNERS:

Regional CIOs/CISOs

TEDCO

NCCoE

Local cybersecurity CEOs

MD TechCouncil

VC/Angels who already evaluate cybersecurity products/ solutions

2 Include cybersecurity (and these recommendations) in MCEDC's new marketing/public relations campaign to raise awareness of the existing cybersecurity community and demonstrate MCEDC's commitment to additional growth.

As part of MCEDC's rebranding and marketing strategy, cybersecurity should be featured as a significant emerging industry in the county.

MCEDC should communicate regional cyber activities, policy developments, capital investments and general industry interests more formally in monthly e-newsletters or through guest contributors' written pieces and interviews. Additionally, through MCEDC's website and social media accounts, Montgomery County-based cybersecurity companies and innovators, in particular, should be highlighted, as well as testimonials from global companies/institutions who successfully use local cyber products.

MCEDC should continue to participate in international events like the annual RSA conference, and regional events coordinated by NCCoE, CAMI, MD Tech Council, the state commerce department and other partners.

To foster relationships among its own nascent cybersecurity companies, MCEDC should host a weekly spring dinner series that offers networking and speakers of interest each week during April and May.

MODEL PROGRAMS:

CAMI

The Cybersecurity Association of Maryland, Inc. (CAMI) is a nonprofit that started in 2015 to operate the Buy MD Cyber program. mdcyber.com In addition to its on-line presence, CAMI has events throughout the year, including the Cyber Day/ Marketplace event, which was recently held at the NCCoE facility in Rockville, MD.

MACH37 Security Leaders Dinners

Mach37 is a cybersecurity accelerator in Herndon, VA. In addition to its 90-day accelerator program, Mach37 hosts weekly dinners, which often have upwards of 100 participants in the local cybersecurity community.

IMPLEMENTATION STEPS:

MCEDC should:

- Work with its marketing team/contractor to feature cybersecurity as an emerging industry.
- Continue to partner with state organizations and NCCoE to create another Cyber Marketplace event for the Spring 2017.
- Begin a cybersecurity weekly dinner series in 2017.

PROJECT COSTS:

This work can be absorbed in MCEDC's existing budget.

PARTNERS:

NCCoE

CAMI

MDTechCouncil

Department of Commerce

Regional incubators, accelerators and work space tenants

3 Create a life-cycle investment fund or board that invests, directly, into local cybersecurity startup companies.

The workgroup agrees with the Amplifier report's conclusion that direct investments in local cybersecurity startups are necessary to strengthen this emerging industry. MCEDC should create an entity that offers a continuum of investments—from seed-capital to Series A, B & C rounds—which supports the entire lifecycle of a young company.

This "lifecycle" approach to investing is particularly important for local cybersecurity companies that don't fit a typical VC model, or are not led by a serial entrepreneur with established ties to the VC community. There is also a noted gap between seed investments and venture capital that needs to be filled.

MCEDC's venture fund should source and evaluate local cyber investment opportunities using business professionals, investors, entrepreneurs and researchers. These experts would find investment opportunities, evaluate proposals, and choose which opportunities to fund.

There are several regional entities that provide some type of funding, although the workgroup agrees with the Amplifier report that existing funding is insufficient to make a substantive improvement to the local cybersecurity industry. For example, the Maryland Technology Development Corporation (TEDCO), Seed Investment Fund provides up to $100,000 in a five-year convertible note (8% interest per year).

MCEDC's cyber-related venture fund efforts should be closely coordinated with other MCEDC investor cultivation activities so that multiple funding requests are not confusing to potential contributors.

MODEL PROGRAMS:

Most privately funded investment programs are angel networks or actual venture capital funds. There are few examples where economic development agencies standup alternative venture funds directed at supporting local businesses. This project will be a design-build endeavor, specific to Montgomery County's needs.

IMPLEMENTATION STEPS:

MCEDC should:

- Identify current administrative funds from MCEDC/Montgomery County/State ($250,000/$500,000) to develop the venture program.
- Work with the MDTechCouncil and legal counsel to determine what type of structure could raise and administer these funds. There are ways for a 501(c)3 to financially support companies, but it needs to be explored more fully.
- Work with its board and other partners to: 1) cultivate local angel investors; and 2) convene prospective investment fund members to outline funding goals, management objectives, etc.
- Work with prospective fund members to create the investment fund business plan and fundraising plan.

PROJECT COST:

$20,000,000 investment capital (private), estimated personnel/administration ($250-500K)

PARTNERSHIPS:

High net-worth individuals with large networks

Angel Capital Association

SBA's Small Business Investment Companies – (3 in Montgomery County)

TEDCO

Dingman Center Angels, Baltimore Angels, etc.

MD TechCouncil

4 Provide policy and legislative guidance to all levels of government regarding the cybersecurity industry.

The workgroup agrees with the Amplifier report's recommendation that coordinating the viewpoints and experiences of cybersecurity businesses, and their clients, is an important component of a healthy industry. MCEDC should provide substantive guidance to all levels of government that reflects the industry cluster's needs. For example, the workgroup believes that state data security breach notification laws impact small businesses disproportionately. Proposed legislation, informed by area cybersecurity experts, could help to alleviate this burden.

Policy coordination can also help with government funding allocations and even related workforce issues. MCEDC's role should be to empower our local industry to find its voice with elected officials and decision makers.

MODEL PROGRAMS:

Advanced Cybersecurity Center, Bedford, MA - A non-profit consortium of private, university, government and non-profit leaders who advance cybersecurity in New England. They focus on research and development, education/talent and advancing public policies. It is worth noting that their focus is on reducing cyber threats, not necessarily growing the cybersecurity industry.

IMPLEMENTATION STEPS:

MCEDC should:

- Create an outreach strategy to local cybersecurity companies that will solicit input on existing and pending legislation and regulations.
- Create an on-line platform, or community, for cybersecurity stakeholders where they can discuss policies and mobilize, as needed.

PROJECT COST:

$25,000-$100,000 per year, per the Amplifier report.

PARTNERS:

Cybersecurity business owners, CEOs

Public Officials

MD TechCouncil

CAMI

5 Develop talent to expand Montgomery County's cybersecurity workforce.

The workgroup members' experiences reflect the report's findings regarding the shortage of cybersecurity talent in the region. MCEDC should support the continued efforts of Worksource Montgomery, Montgomery College, and the Universities at Shady Grove to address this challenge. While MCEDC is not a training organization, it should certainly help educational institutions and relevant organizations connect with both the emerging cybersecurity companies to assess their changing needs, as well as existing companies and anchor institutions.

As MCEDC evolves and expands its capacity, the support of early education programs, like coding in the public schools and other STEM activities may become a priority.

MODEL PROGRAMS:

Cyberworks – Anne Arundel Workforce Development Corporation

Cyberworks is an industry-led program to help job seekers build careers in cybersecurity. Participating business partners provide hands-on training, skill building, and mentorships to pre-vetted candidates for 20+ hours per week. CyberWorks subsidizes the training costs for business partners.

IMPLEMENTATION STEPS:

Follow our partners' lead in determining how MCEDC can best facilitate success within the cybersecurity industry cluster.

PROJECT COST:

This can be absorbed in the MCEDC budget.

PARTNERS:

Industry Leaders

Worksource Montgomery

Montgomery College

Universities at Shady Grove (and its affiliates)