UNITED STATES SENATE

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP

"The Role of Small Businesses in Strengthening Cyber Security Efforts in the United States."

TESTIMONY OF Charles Iheagwara, Ph.D., CISSP, PE

Chief Marketing and Business Development Officer

Unatek, Inc.

Monday, July 25, 2011

Good afternoon. Thank you, Senator Cardin, and members of the Committee for inviting me to testify today on issues pertaining to the role of small businesses in strengthening Cyber security efforts in the United States. Cyber security is a practice I have been engaged in for well-over 10 years now, has meant a great deal to my company, and I look forward to telling you a bit about my experience.

My experience in Cyber security spans different domain areas of practice with big and small firms and federal and state government consulting. As well, I have deep-rooted academic background on Cyber security having written a Ph.D degree Dissertation titled: "The Effectiveness of Intrusion Detection Systems" at the University of Glamorgan, Wales, UK and most recently an MS degree Thesis titled: "The Strategic Implications of the Current Internet Design for Cyber security" at the Massachusetts Institute of Technology (MIT), Cambridge, USA.

Since my professional practice started in January, 2000 as a security engineer at Edgar Online, Inc. (formerly known as Financial Insight Systems) that maintained a significant portion of the NASDAQ IT and technical infrastructure, I can truly say that every day has been a learning experience. Working collaboratively with lines of operations department unit heads and IT security personnel I gained valuable knowledge on the scope and depth of vulnerabilities and high risks that characterize Cyberspace and the essential elements of mitigation approaches.

Additional field experience was gained through my lead consulting roles at Lockheed Martin, KPMG and Aligned Strategies Development Corporation. Also at Unatek, Inc., I have led several client engagements and project implementations delivering Cyber security solutions to federal, state and local governments.

Unatek, Inc. as an Information Technology consulting firm has established a niche in Cyber security solutions and services. Although founded in 1996 as an environmental engineering company, it changed its business line in 1998 to Information Technology

and ever since then has provided Cyber security services to several federal and state government agencies and many public sector organizations. Most recently, Unatek, Inc. was the recipient of the 2011 "Maryland Homeland Security Company of the Year" award (http://thedailyrecord.com/2011/06/03/maryland-incubator-company-of-year-award-winners-named/).

In the last three years, Unatek expanded the scope and range of its Cyber security services and operations to include several niche services in Security Engineering and Architecture, Risk Management and Advisories, Continuous Monitoring, Computer Incident Response and Forensics Investigations, FISMA Compliance, Training, Security Operations to mention but a few.

Current and past clients include the US Department of Commerce, US Smithsonian, US Department of Labor, US Department of Veterans Affairs, US Marine Corps, US Department of Homeland Security and the District of Columbia government. Private sector clients include the Metropolitan Washington Airports Authority, Washington Metropolitan Area Transit Authority, Reagan National Airport, Dulles International Airport, KPMG and Lockheed Martin.

Branding of specialized unique products and services are under way in the company. In the last five years we have successfully incubated and branded a world-wide Cyber security conference and expo suites (http://www.unatekconference.com/intrusion_home.php) that provides the forum for security professionals to collaborate, exchange ideas and transfer knowledge. To date, three (3) events have been organized and plans are underway to make this a permanent feature of our practice. We are also in the process of incubating a Cyber security analyst and online media service that when fully developed, will provide analytic services on the technologies, products and processes that enable Cyber security and the marketplace dynamics that drive growth in the sector.

As a Cyber security company, we are a frontline problem-solver and are constantly at the forefront of technological advances, government policy, envisioning the need for information and operational security, investing in facilities, corporate infrastructure and personnel to expand our service offerings as a highly qualified Information Technology company. Unatek continues to be an early adapter of advanced processes, toolsets, security technologies, and services necessary to support our federal and commercial clients. This coupled with our dedication and commitment has ensured lasting relationships with our government and private clients over the years.

As a small business we have successfully executed on very complex Cyber security projects. For example, we provided niche subject matter expertise for Lockheed's next generation intrusion detection systems. As the Computer Emergency Response Coordinator, our staff directed intra-agency emergency technology for District of Columbia. At the Dulles International and Reagan National Airports, together with our KPMG partner, we provided risk management solutions that mitigated risks and enhanced security at two of our nation's busiest airports.

Leveraging the products and toolsets of our strategic business partners (Juniper Networks, Microsoft Corporation and Cisco Systems) we provided Business Intelligence training to the US Department of Veterans Affairs, multi- track certification training in various networking and security domains to the US Marine Corps in satisfaction of DoD 8570.1 Directives, and FISMA training to the US Department of Homeland Security.

At the US Department of Labor, we provided FISMA and complex Continuous Monitoring support; and Certification and Accreditation support to the US Department of Commerce and the US Smithsonian Institution.

Unatek is also providing very specialized niche Cyber security services to a variety of quasi-government and private sector clients. For example, Unatek is providing specialized PeopleSoft application security support in addition to network security support to the Washington Metropolitan Area Transit Authority. Also in the recent past, we set up a Cyber security lab and trained several Cyber security personnel at the medium-sized audit firm of Thompson, Cobbs, Bazilio and Associates (TCBA), and provided a wide range of consulting services to incubate and nurture their Cyber security practice.

The contributions made by Unatek in helping the nation combat Cyber attacks mirrors those made by countless other small businesses. As a small business, providing Cyber security solutions and services is not always easy due to a variety of reasons primary of which is the limited availability of resources to expand services and market. But, reliance on several factors such as low-overhead, resourcefulness of our personnel, availability of niche expertise within our talent pool, effective management of project execution and a very efficient alignment of corporate resources have been the key to our successes.

Like hundreds of other small businesses, we continue to partner with other business entities in the Cyber security field. We are reseller's of Cyber security products from big-sized businesses such as McAfee, Inc., Juniper Networks, Cisco Systems and small-sized firms such as TransGlobal Business System. We are also constantly pursuing teaming, subcontracting and other collaborative ventures with firms like SAIC, Booz Allen Hamilton (BAH) and others that rely, in no small measure, on small businesses to deliver services and solutions.

All over the country, there is growing evidence that small businesses are playing an important role in the US national and local economic development. SBA data demonstrate that small businesses provide majority of new jobs and produce much of the creativity and innovation that fuels economic progress. On this, Unatek has provided employment to many and every new contract means new employment and additional source of revenue to support growth and expansion of services.

In the national economy, small businesses are the employees, the customers and the suppliers who provide goods and services to the federal, state and local Cyber security markets. They also provide significant, if not the majority, of the entrepreneurship that

drive growth in the Cyber security market space. Many of them are entrepreneurial and come from innovation-oriented academic institutions such as MIT and Stanford where thousands of small businesses have been launched by current graduate students or recent graduates. Many of these small businesses have become centers of innovative and entrepreneurial ventures where technological groundbreaking is a regular feature.

The growth of many medium and big-sized firms is made possible by the entrepreneurship of small businesses. Thousands of these companies have peaked in their organic growth but continues to grow from mergers and acquisitions of highly entrepreneurial small businesses. Therefore, there is no doubt that the entrepreneurship of small businesses is the fuel that propels growth, consolidation and expansion of services in organizations that have peaked in their organic growth. In the last ten (10) years, it is worthy to note that countless numbers of small businesses that are in the Cyber security business have been acquired by large firms.

The role played by small businesses in strengthening Cyber security efforts in the United States can be measured by several metrics and indicators. But by most accounts, the impact of small business contributions to the Cyber security sector and the overall economy can be described in the broad terms of "Talent," "Capacity Creation," "Incubation," "Innovation," "Niche Services" to mention but a few.

1. **Talent** – Cyber Security is a field that has become highly specialized. Like the medical profession where there are general practitioners and specialists, in the Cyber security practice, we have those that specialize in Policy work, Certification & Accreditation, Security Engineering and Architecture, Analysts, etc. Small businesses with lower overhead structures are sometimes more capable of attracting and retaining niche talent.

2. **Capacity Creation** – Many Cyber security initiatives at the federal and state levels spur capacity creation of different business lines and activities. A case in point is the recent DFAR changes proposed by the DoD that will affect the entire DoD supply chain which consist of mostly small businesses. Creating services that these small companies can use will become extremely important (and lucrative for the companies that do it).

3. **Incubation** (of Technologies, Business Processes and Practices) -

   Many Cyber security technologies, business processes, toolsets to mention but a few were incubated by one or a group of individuals working as small business entities that are engaged in Cyber security practice or elsewhere. Such incubations eventually grow into products, solutions and niche services that are eventually launched into the market place by the big companies that acquired them.

   In multiple instances, in one form or another, the concepts and ideas behind many Cyber security defense arsenals like the firewalls, intrusion detection

systems, virtual private network devices, etc. originated from small businesses or individuals who are practicing as independent consultants.

4. Innovation

Small businesses are often executors of complex projects. As prime contractors, subcontractors, independent consultants and employees they are central to ideas generation. Through the many complex projects they work on they often discover areas of process, product, toolsets, business process and technology that need improvement. For example, as lead users of business toolsets, small businesses often recognize deficiencies and go on to improving or innovating the toolsets. They can be viewed as a poster child for the concept of "user innovation" as defined by MIT's Eric von Hippel or "crowdsourcing" as coined by Jeff Howe in a June 2006 Wired magazine article about istockphoto (http://www.wired.com/wired/archive/14.06/crowds.html). In contrast to the traditional R&D model that characterize big firms' innovation machines, where billions of dollars are spent before anything meaningful comes out of the efforts, working on the frontline, small businesses are better at collecting customer inputs to innovate, a move away from the traditional R&D to where users drive innovation.

Small business driven Innovation come in different shades. "There are a lot of different things that fall under the rubric of innovation," says Vijay Govindarajan, a professor at Dartmouth College's Tuck School of Business and author of *Ten Rules for Strategic Innovators: From Idea to Execution*. "Innovation does not have to have anything to do with technology." In the 1990s, innovation by small businesses in the Cyber security market space centered mostly on developing the technologies, quality control and cost of addressing Cyberspace threats. Today, in consonance with the nature of Cyber security which has become a constantly shifting target, small business driven innovations now revolve around efficiency and rewiring them for creativity and growth. For example, Sourcefire, Inc. that developed one of the model intrusion detection systems was until a few years ago a small Cyber security firm. It created the "Snort" that was a basic model for intrusion detection systems. Today, it is a publicly traded company with many leading-edge Cyber security products. In the nineties when Snort was created, technology development was the main focus in the Cyber security market. Today, innovation has moved beyond defining the technology onto some other forms of perfecting existing technologies and products, improving techno-economic efficiencies and cost of operations among others. This is generally reflective of the trend across the industry and the contributions by small businesses in different innovative endeavors are by no means small in comparison to those that originate for big-sized Cyber security organizations.

Inherently, across the field, there are small businesses evoking all types of innovation. There are technology innovators, business model innovators, process innovators amongst other.

5. Niche services

Niche services are those services that require specialized expertise, setup and organization to deliver. The expertise is largely acquired outside the bounds of any formal or organized training organization. The most recognized niche service in Cyber security is ethical hacking services. Although many training institutions deliver some form of Cyber security training with ethical hacking content, it is known that ethical hacking expertise is largely acquired through other means that are outside the confines of a trainer classroom. The most famous hacker Kevin Mitnick did not acquire his hacking skills in the classroom but rather through his extraordinary talent. Today, individuals with such talents have organized their practice around small business consultancies that provide their highly specialized services to hundreds of big businesses, the defense and Intelligence establishments and others that are in constant need of testing their information systems for proof of resistance to hackers.

Today's burgeoning niche services have become business requirements arising from different needs. In some cases, the need arise unexpectedly where such services have not yet being incubated, matured or fused into organizational business units and outside the reach of the entity requiring immediately service. Organizing for service delivery then becomes a long term project and the immediate recourse is to small businesses that have the established capabilities to organize and deliver them. In Cyber security field practice, we have seen countless such situations where the big companies working as prime contractors are not able to provide certain niche services but rely on small business subcontractors or independent consultants to provide them. Inherently, niche expertise is a mainstay in small business day-to-day existence.

Given the above, it could be argued that the key elements in Cyber security development strategy is to focus on the strengths and core competencies of small businesses that will enhance the overall security posture of our nation. There will be much value in examining ways to strengthen Cyber security efforts in the United States especially examination of the dynamics that drives innovation and spurs growth in small businesses with good track records and viable potentials. These could very well be the spark that unleashes the innovative fire in small businesses engaged in Cyber security practice.

Despite the very strong and positive contributions of small businesses in strengthening Cyber security efforts in the US, there are still obstacles in realizing the full potentials of small business entrepreneurship. Like individual entrepreneurs and big businesses, they require government support.

With a supportive environment and a fully committed program, both legislative and otherwise, small businesses can continue to grow, expand and drive Cyber security efforts towards new heights. The government, in its efforts to support small businesses in Cyber security, should address obstacles that prevent them from increasing their contribution to the overall economic growth of the USA.

Such programs should provide high quality initiatives that are supported by a legislative mandate and should stipulate a certain percentage of small business share of all federal contracts awarded for Cyber security. Low interest loans to support innovation or niche projects will strengthen the managerial skills of prospective and current small businesses and assist them in selling their products and services to the government. The program should also facilitate access to information, counseling and new Cyber research initiatives.

Before I close, I want to thank Senator Cardin again for asking me to testify. I gained my U.S. citizenship in May, 2006, and I am honored to be recognized for my company's success, and to represent American Small Business entrepreneurs everywhere. I will be happy to answer any questions the Committee might have.