GTSConnection

Advocating for small and mid-sized companies in the Federal homeland and national security market

DHS Should Seize Opportunities Posed by Sequestration

I was on a planning committee meeting for a major technology conference focused on homeland when one of the participants said, "well this conference probably won't be around next year." I was shocked – and frankly dismayed – at the number of organizations and companies giving up on homeland security.

A combination of budget decreases, longer and longer award cycles and a lack of substantive engagement by some DHS components has made the homeland market increasingly unpalatable. The conversation between many of the components of DHS and the private sector has faltered and it's hurting the mission of securing the homeland. Yet—as the recent active shooter incident at the Naval Yard in Washington, D.C. indicates—we have so much work to do. And we need to put politics aside and work more closely than ever before to leverage the opportunities for information exchange, team work and community that exist through so many organizations and networks.

To track the impacts of sequestration, GTSC surveyed YOU earlier this year and the results are telling:

• Almost 30% of respondents – for the most part emerging and small companies - think they may not or definitely will not survive sequestration

• 54% of respondents believe sequestration will materially impact the ability of their Federal clients to conduct their stated missions

• Respondents believe the long-term effects include: weakening of national security and preparedness, uncertainty about the Federal market, loss of skills and experience in vital missions, and increased efficiency

• Respondents believe the short-term effects include: uncertainty, distraction from the mission, loss of jobs and decreased morale

• Companies are preparing by reducing their marketing budgets (29.8%), laying off staff (26.7%), reducing public relations budgets (22.7%), cutting services (19.6%), leaving the Federal market (18.7%) and bringing services in-house (15.6%)

The survey shows that the risk of sequestration and budget cuts is two-fold: you have a number of companies that may not survive and you have numerous mission critical agencies that are at risk as well. Now more than ever we need the government and industry working together to assure mission success to find convergence points where we can make strategic cuts and still protect the nation.

To read more about the survey, visit www.gtscoalition.com/sequestration-survey.

Kristina Tanasichuk is the Chief Executive Officer of the Government Technology & Services Coalition. She is also president and founder of the organization, Women in Homeland Security.

CTP Uses Agile Development to Cut Resource Burn Rates & Delivery Time

Chameleon Technology Partners (CTP) has worked big data since the 1990's for Fortune 50 Companies as well as the Federal government. This enterprise experience enables us to assess situations efficiently and make immediate impact to the development of IT systems. Our support of Federal efforts include the DoD-Financial Accounting Systems (DFAS) Business Activity Monitoring (BAM)—a heterogeneous data warehouse of over $300B worth of annual contractor transactions analyzed for fraud and waste—with over $14M On-line Transactional Processed (OLTP) records processed monthly.

For the Office of Secretary of Defense (OSD), one of the challenges of the project was that the task order contract was sold as a traditional waterfall approach to Systems Engineering Life Cycle (SELC) development of IT systems. However, the needs of the client required an Agile development approach. We immediately reformulated our life cycle approach and were able to cut resource burn rates by 35%. In addition, we implemented a rapid application development (RAD) approach to the SELC while deploying a CMMI/development continuous improvement approach that decreased delivery from three months to four-week cycles. Development teams were re-organized from purely functional teams to matrix teams of multiple capabilities to provide the needed overlap and cross training necessary for team members to understand the full picture of what was delivered from data quality to user interface development and database administration.

Our business category may be small but our client value is Big Data. See us at www.ChameleonTechnologyPartners.com

By John H. Pan, President, Chameleon Technology Partners

Cybersecurity Awareness Month Programs

OCT 3 **Key Cybersecurity Issues for Government Contractors** Brian Finch, Partner, Dickstein Shapiro & Justin Chiarodo, Partner, Dickstein Shapiro LLP

OCT 10 **Cybersecurity Acquisition: What is the Government Buying?** Brian Finch, Partner, Dickstein Shapiro LLP & Graham (Rusty) Mathews, Senior Legislative Advisor, Dickstein Shapiro LLP

OCT 16 **Mentor Session:** Harris Corporation
Keith Bryars, National Security and Federal Law Enforcement, Harris Corporation

OCT 23 **Cybersecurity Awareness Month Program**
Co-hosted with the InfraGard National Capital Region Members Alliance

OCT 25 **Insight Session:** Robert Carey, Principal Deputy CIO, DOD

Register for these and other upcoming programs: www.gtscoalition.eventbrite.com

Take the Cybersecurity Survey

GTSC has partnered with the InfraGard National Capital Region Members Alliance to research the private sector's awareness, understanding, preparedness and gaps related to cybersecurity intrusions and attacks. The results will provide the basis for enhancing or initiating efforts to strengthen the information sharing and awareness to inform our public private partnerships and create meaningful programming and tools to combat cyber threat.

INFRAGARD MEMBERS ALLIANCE NATIONAL CAPITAL REGION

Cybersecurity Survey link: www.gtscoalition.com/cyber-survey

Ten Cyber Issues Board and Chief Legal Officers Need to Know (and Worry) About

Dickstein Shapiro LLP, GTSC's Strategic Partner, recently published this article on our blog. We have summarized the key points here. For the full article, please visit: www.gtscoalition.com.

Boards of Directors have several fiduciary duties to uphold. Meeting such duties requires addressing cybersecurity and data loss. While this rapidly evolving area has its own unique challenges, boards, as well as the legal officers who advise them, face the same question about how to address cybersecurity, data loss, and data theft as they do any other critical issue-are they acting prudently, reasonably, and responsibly? More and more boards are now asking themselves, and the legal counsel who advise them, these questions and placing cybersecurity and data theft risks at a higher level of priority than even physical disasters. The factors highlight 10 areas boards and their legal advisors should consider before their companies are faced with a real-world cyber threat:

1. The stakes to share value and the bottom line are high.
2. The hackers are two steps ahead of you already.
3. Cyber and data loss threats pose merger risks.
4. Lost or stolen intellectual property or customer or employee information can turn a deal from sweet to sour.
5. There is a maze of state and Federal data protection and data loss notification requirements to navigate.
6. The failure to be fully informed of and proactive against cybersecurity and data loss risks could lead to litigation.
7. If the breach doesn't get you, the litigation will.
8. There are Federal programs available to help mitigate corporate liability through the SAFETY Act.
9. Insurance coverage is available through traditional or tailored policies.
10. Outside counsel comes with the benefit of attorney-client privilege.

DICKSTEINSHAPIRO LLP

By Divonne Smoyer, Brian E. Finch (pictured) & Emanuel Faust Partners, Dickstein Shapiro LLP

Scan to sign up for GTSC's Weekly Insider for upcoming programs and news!

Robert Carey, Principal Deputy CIO, DOD on Cyber & Innovation

GTSC: Everyone is talking about cyber — what does this mean to you?

RC: "We (DOD) are faced daily with escalating rounds of exploits and attacks of our networks and systems. Our approach to cyber is primarily defensive, but we have the ability to defend the nation as required. The Defense Information Systems Agency (DISA) manages the defenses of DoD Networks working alongside and in support of U.S. Cyber Command who is standing up teams that will operate and defend our networks and the nation's interests in cyberspace.

In the defensive arena, we are focused on inculcating identity management for the user, deploying a layered security approach that connects from the Internet gateway to the desktops (and mobile devices) and innovation that can help evolve with the threats."

GTSC: You also hear the word "innovation" thrown around a lot. When a company says it has an "innovation," what are you looking for?

RC: "Proof. I'm looking for facts and data. There are very few technologies that pass through that "don't work." What I'm looking for are the data that support a company's claim of innovation, an understanding of success rates and even some case studies or business case analyses of where the innovation has worked. The conversation often gets pretty silent when I start drilling down for more technical answers or actual examples of the innovation at work.

As far as the threats go – we all read about new ones every day. We are probed and scanned constantly and we need to find evolving security measures that work on both the human and technological vulnerabilities."

GTSC: So what is your advice for small and mid-sized companies who believe they have a solution for one of your challenges?

RC: "Do your homework on the Department, its size, depth, breadth and purpose. I know everyone says that a lot, but I need folks who have spent some time getting to know the Department, understanding what we do, what we need and why. We need executives who can match their technology or innovation to a problem we have, show me how they can fix it and provide real-world data on success rates, within budget constraints."

JOIN GTSC *on October 25 to hear from Robert Carey*

Advocating for small and mid-sized security companies in the Federal marketplace

GTSC Government Technology & Services Coalition

ITS ABOUT THE MISSION

Join us today at www.GTSCoalition.com

@GTSCoalition
Facebook.com/GTSCoaliton
LinkedIn
www.gtscoalition.com/blog

Government Technology & Services Coalition
For more information, contact:
membership@gtscoalition.com

Government Technology & Services Coalition. GTSC is a 501(c)(6) nonprofit, non-partisan association of companies that create, develop and implement solutions for the Federal homeland and national security sector. Our mission is two-fold: first, to provide exceptional advocacy, capacity building, partnership opportunities and marketing in the Federal security space for small and mid-sized companies. Second, to support and assist our government partners achieve their critical missions with the highest integrity; best and most innovative technologies; and results-based, quality products and services to prevent, protect against, mitigate, respond to and recover from any terrorist attack or natural disaster. For more information on these mentors and the Government Technology & Services Coalition, please visit www.GTSCoalition.com.