Contact:

Kevin DeSanto
KippsDeSanto & Co.
703.442.1402
kdesanto@kippsdesanto.com

www.KippsDeSanto.com

Ensuring Cybersecurity in the Next Administration

By Kevin DeSanto and Aaron Sharp

With such significant focus on the economy and bailout packages, little mainstream attention has been paid to one of the largest issues facing the Obama administration: cybersecurity. Malicious information theft, disruption and denial have the potential to cripple the very foundation of U.S. infrastructure and everyday life. Network and system vulnerabilities have compromised national and economic security and have already been exploited in cases ranging from massive power blackouts affecting tens of millions of Americans to multi-billion dollar intellectual property thefts from prominent U.S. Government agencies.

Critical Issues for the New President

Organizations from a multitude of industries have already presented their case for assistance during this transition of administrations, but weaknesses in cybersecurity could present an equivalent if not far greater threat to the country than the current economic environment – the "what ifs" are innumerable.

The U.S. Government is fraught with network security holes. Melissa Hathaway, Cyber Coordination Executive for the Director of National Intelligence, has detailed the ambitious program to reduce federal enterprise access points from thousands to less than 100. Programs such as the Bush administration's Comprehensive National Cybersecurity Initiative and the Department of Homeland Security's Einstein Program have only begun to stem the tide already hitting federal networks. A now very public example highlighted in BusinessWeek is the case of NASA, where numerous digital intrusions have resulted in the theft of technology that cost U.S. taxpayers $1.9 billion to develop, in addition to priceless intellectual property "gleaned from the last 50 years of rocket engine development in the U.S." according to an internal NASA memorandum. In fact, President Obama has already been the victim of a sophisticated cyberattack. In the run-up to the general election, the campaign networks of both Senators Barack Obama and John McCain were infiltrated. The FBI and Secret Service investigated and determined that an unnamed foreign entity was the culprit.

Cybersecurity vulnerability is not a problem isolated to the U.S. Government. Following the relocation of an Estonia-based Soviet World War II memorial in late April 2007, Russians were accused of launching a distributed denial of service ("DDoS") attack on Estonian Government websites that forced many agencies to shut off access to IP addresses from outside of Estonia for several days. A DDoS attack attempts to make a computer resource unavailable to its intended users, often by covertly conscripting outside computer resources to carry out the attack. Various sources estimate that as many as 10% of all computers in the world have been used to carry out DDoS attacks. In the weeks leading up to the recent conflict with Georgia, Russians were accused of a DDoS attack targeting several Georgian websites including the website of Georgian President Mikhail Saakashvili and the National Bank of Georgia (*New York Times*).

A potentially weaker link in U.S. cybersecurity is the commercial, specifically financial, sector. As pointed out in a December report by the Center for Strategic and International Studies, the private sector in the U.S. and other market economies plays a significant role in the design, deployment and upkeep of critical infrastructure; so unlike traditional national security assets such as tanks and planes, cybersecurity cannot be provided solely by the government. While phishing, a form of hacking often employed to steal personal information such as credit card numbers, is an important threat to recognize, a DDoS attack on a major financial institution could be devastating. Director of National Intelligence Mike McConnell has stated that 95% of the cybersecurity threat is a private sector problem and cybertheft accounts for as much as $100 billion in annual losses to the American economy (*The New Yorker*).

Cybersecurity Market Opportunities and M&A Activity

According to Input, U.S. Government spending to secure military, intelligence and other agency computer networks is forecasted to grow 45% from $7.4 billion in 2008 to a projected $10.7 billion in 2013. Major defense contractors have taken steps to advance their cybersecurity capabilities – Boeing setup its Cyber Solutions division in August, Lockheed Martin launched its cybersecurity division in October (*Bloomberg*) and Raytheon plans to add 300 more security engineers in 2009 in addition to the two computer network security firms it acquired in 2008. Smaller firms are also positioned to receive an increasing amount of work in the cybersecurity space as they are often more nimble and innovative and can provide expedited solutions drawn from commercial and proprietary sources.

Acquisition activity in the cybersecurity arena is expected to be strong as the larger contractors are eager to expand their expertise in the space and recognize that there is a large stable of newer firms with unique capabilities and knowledge already working on solutions for the cybersecurity threat. M&A activity in the cybersecurity space will likely continue to trend toward more of the commercial / government capability convergence that is being witnessed across the government contracting space as

a whole – traditionally commercial companies will play a significant role as acquirers and create greater competition for traditional government contractors. In addition, these traditional government contractors will need to look more broadly at commercial acquisition targets in order to develop the capabilities required by their customers. This will be driven in large part by the complexity and urgency of the cybersecurity threat. The following table highlights select cybersecurity deals that have been announced in the past 12 months.

Select Cybersecurity M&A Transactions

Announce Date	Buyer	Seller	Seller Location
01/12/09	Vector Capital	Aladdin Knowledge Systems Ltd.	Petach Tikva, Israel
01/05/09	CA, Inc. (fka Computer Associates)	Orchestria Corp.	New York, NY
11/28/08	ManTech International Corp.	EWA Services, Inc.	Herndon, VA
10/08/08	Symantec Corp.	MessageLabs Group Limited	Gloucester, United Kingdom
09/30/08	VMware, Inc.	Blue Lane Technologies, Inc.	Cupertino, CA
09/21/08	McAfee, Inc.	Secure Computing Corp.	San Jose, CA
08/31/08	McAfee, Inc.	Lockdown Networks, Inc.	Seattle, WA
08/31/08	Proofpoint, Inc.	Secure Data In Motion, Inc.	San Mateo, CA
08/27/08	Secure Computing Corp.	Securify, Inc.	Cupertino, CA
08/18/08	Symantec Corp.	PC Tools Pty Ltd.	North Sydney, Australia
07/31/08	McAfee, Inc.	Reconnex Corporation	Mountain View, CA
07/29/08	Help / Systems, Inc.	PowerTech Group, Inc.	Kent, WA
07/28/08	Motorola, Inc.	AirDefense, Inc.	Alpharetta, GA
07/28/08	Raytheon Company	Telemus Solutions, Inc.	Falls Church, VA
07/15/08	NitroSecurity, Inc.	Ripple Technologies, Inc.	Conshohocken, PA
07/11/08	Thales Group SA	nCipher Corporation Ltd.	Cambridgeshire, United Kingdom
06/17/08	Fortinet, Inc.	IPLocks, Inc.	San Jose, CA
04/28/08	Phoenix Contact GmbH & Co. KG	Innominate Security Technologies AG	Blomberg, Germany
04/18/08	Raytheon Company	SI Government Solutions, Inc.	Melbourne, FL
04/04/08	EMC Corporation	WysDM Software, Inc.	New York, NY
02/28/08	SafeNet Inc.	Ingrian Networks, Inc.	Redwood City, CA

On March 20th, the Bush administration named Rod Beckström head of the National Cyber Security Center. In this role, Beckström will be the country's top cybersecurity watchdog and lead the recently created interagency group. The choice of Beckström, a Washington outsider who made his name as a Silicon Valley serial entrepreneur, suggests the federal government recognizes the cyberthreat as a clear and present danger requiring innovative technologies to be delivered quickly. Indeed, cyberattacks on federal networks have increased approximately from 30,000 in 2007 to 70,000 in 2008. This current level of cyberattacks has been equated by senior leadership in the U.S. Intelligence Community to a cyber Katrina, except that the public is oblivious to the carnage. Beckström and the new Obama administration face enormous challenges including increasing public understanding of the scope of the problem, decentralizing bureaucracy and minimizing procurement obstacles standing in the way of successfully securing federal and commercial networks from cyberthreats. The "$64 billion" question is: will the government succeed?