VECTIS STRATEGIES

The Value of Bipartisanship

About Vectis

Vectis is the Latin word for “leverage.”

At Vectis Strategies we understand how to successfully and properly apply leverage in public relations, government affairs and business development. It’s done through utilizing our bipartisan, deep and longtime relationships that stretch from the corridors of power in Washington, DC to international agencies, state houses, city halls, local communities and newsrooms nationwide. The founders of Vectis Strategies have a proven and respected track record for historic accomplishments through bipartisan collaboration. Our clients understand that nearly every issue is “political” to one degree or another. We understand this as well and have successfully navigated the political landscape building legendary bipartisan support around complex issues for decades.

The founders of Vectis Strategies have served in roles as diverse as high-ranking Members of Congress, the Chairman of a U.S. Presidential Campaign, Chairman of the California Democratic Party to a Mayor in San Diego County, a senior executive of one of the Nation’s “Top 10” PR firms and as Chief Corporate Officer of a multi-national company.

Headquartered in California, with offices in Los Angeles, Sacramento, San Diego and Washington, DC, Vectis Strategies is the only firm with founders from both sides of the aisle that have longtime bipartisan ties with the California Congressional Delegation, the largest in the United States.

The Value of **Bipartisanship**

Cyber Strategic Initiative

Our interdisciplinary Cybersecurity team is at the forefront of cybersecurity issues. We advise on all aspects of government affairs, government contracts, corporate, IP, and litigation including developing compliance programs to prevent attacks, conducting breach response plans, advising on compliance and risk management, and cultivating effective government relations strategies.

Changing Landscape

- Companies are facing a constantly changing landscape (with regards to addressing cybersecurity issues), which includes: the White House executive order and legislation; evolving regulatory requirements; increases in penalties and fines; and, liability from class action lawsuits.

- In order to minimize risk, it's important to keep abreast of changing transatlantic requirements as they are being proposed so that you have the opportunity to affect the process.

Why Should You Care?

- In most sectors, cyber used to be the responsibility of the firm's tech/IT point person/CISO, but now in recognition of the liability that cybersecurity carries, it has become a "c-level" issue.
- We face a persistent sophisticated threat and a determined adversary.
- So why should you care and how do you elevate cyber?
- Your data, your IP, and your reputation are at risk.
- Are port authorities involved in elevating cyber to your leadership and creating best practices in the event of a cyber attack?

The Big Picture in the United States

- "Cyber Security is a matter of national and economic security." President Obama.
- International Cybercrime nets more revenue than narcotics.
- Espionage-Chinese hacking into your corporate network.
- Every company has been penetrated-80% do not know it.
- Your network is compromised; there is no silver bullet.
- What's most important and what are you doing to protect it?
- Congress and the White House want to do something with increased focus on sectors traditionally more concerned with physical security.

Case Studies

- Cyber espionage is seen as a direct threat to US economic interests- $25 billion to $100 billion in losses.
- Saudi Aramco network attacked by Shamoon virus- compromised with a loss of over 30,000 laptops.
- Initial target was an industrial system .
- New York times attacked by the Chinese-Mandiant report.
- DHS identified an unidentified US power plant that was crippled for week by cyber attacks.
- 2012 US National Intelligence estimate identifies China as the nation most aggressively seeking to penetrate US corporate systems and networks.

Obama Executive Order

- Covers critical infrastructure-February 12, 2013
- http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity .
- The National Institute of Standards and Technology has initiated a process where industry and the federal government will create cybersecurity standards.
- First meeting in early April, next meeting end of May, report in October.
- DHS will turn the voluntary program into completion.

Designated Critical Infrastructure Sectors

- Presidential Policy Directive Critical Infrastructure Security
- http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil .
- Chemicals; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense; Emergency Services; Energy and Electric; Financial Services; Food and Agriculture; Government Facilities; Healthcare; Information Technology; Nuclear Reactors; Transportation; and Water and Wastewater systems.

Focus on Critical Infrastructure

- What happens at your port authority if you get hit by Shamoon?
- Who takes the fall?
- How are you mitigating your risk?
- Are you educating Congress and the White House?
- Sectors like water, electricity, and chemical where the emphasis has been on physical security are now the focus of additional cyber regulation.

Contact Information

Dan Caprio

dcaprio@vectisstrategies.com

202-680-4538

www.vectisstrategies.com