

Written by a Chinese general over two thousand years ago, Sun Tzu's Art of War continues to influence military, political, and business strategy.



Sun Tzu's View of the Cyberspace Policy Review

By Steven F. Fox – ISSA member, Motor City (Detroit), USA Chapter

Leadership from the top – this is the message conveyed by the Obama admin-

istration's Cyberspace Policy Review (CPR). This plan calls for the creation of a cybersecurity coordinator responsible for "orchestrating and integrating"¹ related policies. While operational and tactical details are pending, the strategic focus on communication is a positive step.

While Sun Tzu supported a strong central leadership, he stressed that the government must delegate authority to those on the battlefield. According to Sun Tzu, "those whose Generals are able and are not constrained by their governments are victorious."² In this case, leaders who report to a central authority are the "generals."

Sun Tzu points out that "military and civil affairs are different, dealing with different matters." According to the CPR, the cybersecurity coordinator will prioritize cybersecurity issues at the national level. Melissa E. Hathaway's comment shows that the strategic focus of the plan will "transcend the jurisdictional purview of individual departments and agencies because ... no single agency has a broad enough perspective to match the sweep of the challenges."³

Since this plan transcends the needs of individual government interests, will this apply to private companies? Since 80% of critical infrastructures are pri-

vately controlled,⁴ the unique risk profile of these companies is important. Sun Tzu highlights three ways in which a government can cause problems in their oversight of leaders.

1. When the government mandates a change in strategic direction or tactical decisions that are inappropriate in light of operational factors

The government cannot respond to an incident with the same speed and efficacy that a private company can. This is partly due to the higher number of incidents in the private sector. Given the financial impact of an incident, proper response and recovery is a priority. While most companies have a security policy, the CPR is evidence of the government's continued struggle with a unified stance on information security.

This policy must enable the agility of the private sector while positioning the government as a center of knowledge and guidance. While cybersecurity has an infrastructure component, the unique business environment in which the risk resides must be taken into account.

2. When a government shares authority with C-level leadership but is ignorant in the business affairs that drive these decisions

According to Sun Tzu, "when there are among the civilian officials attached to military commands those who do not know about military leadership, then the chain of command will not be unified, and the soldiers will become hesitant." Staff, system administrators, managers – all these stakeholders must follow a knowledgeable, unified leadership. Thus, the government should delegate all relevant authority to those companies.

Delegation of appropriate authority to private sector leaders is needed since "the cybersecurity policy official should not have operational responsibility or authority, nor the authority to make policy unilaterally."⁵ This official will have to get buy-in from different agencies, coordinate policy and procedures across the federal government, work with the legislative aspects of a given initiative, and ensure that it falls within the president's budget before anything happens. Given the time-sensitive nature of private industry security priorities, the time associated with this process is unacceptable.

3. When the philosophy of civil leadership is applied to the leadership of private corporations

"A nation can be governed by humanity and justice, but not an army. An army can be guided by maneuvering, but not a nation." Sun Tzu realized that the factors involved in governing a nation are different from those of leading a company. Thus, the government must take into account these differences when creating programs to aid companies in the realization of their security strategies.

The Obama administration is heading in the right direction. I hope to see detailed plans that enable the agility of both government and private sector practitioners.

About the Author

Steven F. Fox is the principal consultant for SecureLexicon LLC. He serves on the board of the Detroit ISSA chapter. His Security Paradigms blog appears on www.csoonline.com. Mr. Fox holds a Masters in Business Information Technology from Walsh College. He can be reached at sfox@securelexicon.com.

1 Cyberspace Policy Review, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

2 All Sun Tzu quotations from Thomas Leary, *The Illustrated Art of War* (Shambhala Publications, Inc., October 12, 2004).

3 Melissa E. Hathaway, comments at RSA Conference, April 2009.

4 Daniel Ward and Michael Grimaila, "Who Shall Defend Us? Determining National Defense Roles in the Internet Age." *ISSA Journal* (March 2009).

5 *Cyberspace Policy Review*