Evaluating Your Cyber-Intelligence

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

Long-time readers of this column may recall that I wrote about Rob Rosenberger in 2003 as he was heading for duty in the Iraq war. Rob runs SecurityCritics.org and I’m always happy to receive articles from him. Here’s an interesting piece that he sent me as part of a correspondence with a colleague; he has very kindly allowed us to publish this edited version.

* * *

There is a growing market for cyber-intelligence among companies, governments, and militaries. But there is also an old saying in the intelligence community: "Bad intel is worse than no intel at all."

Are you getting bad cyber intelligence? Is there some sort of litmus test we can apply?

The answer is yes: there is a simple two-part litmus test for any intelligence product.

First, does your cyber-intelligence include dossiers on key members of the computer-security-industrial complex? Second, does your intelligence analysis reveal important issues that are embarrassing or even taboo?

Intelligence firms must never dismiss the need for dossiers on the good guys. Why? Because we cannot know our own strengths and weaknesses until we know those of our allies. The U.S. CIA keeps a dossier on Britain's Air Chief Marshall Sir Glenn Torpy – and Britain's MI5 keeps a dossier on Air Force Chief of Staff General T. Michael Moseley.


Ask your cyber-intelligence vendor for a detailed dossier on your antivirus vendor. Ask for a dossier on renowned antivirus expert Costin Raiu.< http://www.kaspersky.com/virusanalysts#h >
If your vendor keeps dossiers only on the bad guys, then they've failed the first part of the litmus test.

Now let's discuss the second part of the litmus test. Suppose you obtain a dossier on your antivirus vendor. Do they license their antivirus technology from another company? Does it reveal embarrassing or even taboo activities at the firm? Does the dossier offer detailed biographies on major research and development team members? Does it provide a comprehensive bibliography for source information? Does the dossier plagiarize another agency's research?

Intelligence firms must never dismiss the need for the whole truth. Why? Because a partial truth
is actually a lie by omission. Intelligence firms get paid to deliver information, not to withhold it. We learned this lesson the hard way on 9/11/01.

Dissect the dossier on your antivirus vendor. If it contains only news stories, press releases and Gartner Group's short-term assessment of the firm, then it fails the second part of the litmus test. Dissect the dossier on renowned expert Costin Raiu. If it fails to include what I said about him in 2006 in a speech where I predicted that a foreign intelligence agency will oversee nearly all corporate antivirus research by 2010 (video < http://vmyths.com/mm/rants/2006/0808/part02.m3u > or audio < http://vmyths.com/mm/rants/2006/0808/02.mp3 >), then it fails the second part of the litmus test. It's that simple.

Now it's time to put YOU to the test. Let's suppose you realize you've subscribed to poor intel for all these years. Your CIO pays you to give him good cyber intelligence. Will you reveal this truth to your CIO – or will you lie by omission?

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.msia.norwich.edu > at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2006 Rob Rosenberger & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.