Captain Obvious here, bringing you a Public Service Announcement. Your corporation is very likely under attack from cyber-criminals seeking to steal protected information. If you are a government contractor, it is important that you take strong measures to secure that protected information. A failure to secure protected information may lead to lawsuits, degradation of the brand reputation … or worse.

Of course, this is not news to the long-time readers of this blog. We started writing about cyber-warfare and cyber-security in November, 2009. A couple of months later, we discussed the Comprehensive National Cyber Security Initiative (CNCI). A couple of months after that, we posted **an article** in which we warned readers that "cyber protection may become a contract compliance issue." We wrote, "companies will need to comply with the requirements of the new contract clauses, or else risk accusations of breach of contract (or worse)."

A few months later (November, 2010), we added some scare stories about the threats and what happened when cyber-security flaws were exploited. In that same month, another article asserted that, "Your company likely is not enough to secure its computer networks, not nearly enough." In June, 2011, we devoted an **entire article** to "cyber-wars." In that article, we discussed cyber-attacks on Lockheed Martin, Northrop Grumman, and L-3 Communications. And we aren't even mentioning the articles we devoted to the travails of SAIC in this area.

Meanwhile, DOD promulgated a final rule that requires "defense contractors to incorporate established information security standards on their unclassified networks and to report cyber-intrusion incidents that result in the loss of unclassified controlled technical information from these networks."

To sum up, your company has had plenty of time to invest in cyber security and to protect important information. You have seen other companies attacked and you have seen your Government customers create regulatory requirements that provide both carrots (competitive advantage) and sticks (potential breach of contract claims) for those that fail to take the matter seriously enough.

At this point, it's on you.

Accordingly, nobody should be surprised that both Department of Homeland Security (DHS) and the Office of Personnel Management (OPM) have suspended "most contracts" with the government contractor USIS—the self-proclaimed "leader in Federal background investigations."

What happened?

On August 6, 2014, the company issued the following **press release** :

Our internal IT security team recently identified an apparent external cyber-attack on USIS' corporate network. We immediately informed federal law enforcement, the Office of Personnel Management (OPM) and other relevant federal agencies. We are working closely with federal law enforcement authorities and have retained an independent computer forensics investigations firm to determine the precise nature and extent of any unlawful entry into our network. Experts who have reviewed the facts gathered to-date believe it has all the markings of a state-sponsored attack.

Cybercrime and attacks of this nature have become an epidemic that impacts businesses, government agencies, and financial and educational institutions alike. … Our systems and people identified this attack, and, in response, we are working alongside OPM, the Department of Homeland Security (DHS) and federal law enforcement authorities in redoubling our cyber security efforts. We are working collaboratively with OPM and DHS to resolve this matter quickly and look forward to resuming service on all our contracts with them as soon as possible. We will support the authorities in the investigation and any prosecution of those determined to be responsible for this criminal attack.

The Washington Post **reported** —

A major U.S. contractor that conducts background checks for the Department of Homeland Security has suffered a computer breach that probably resulted in the theft of employees' personal information … it is unclear how many employees were affected, but officials said they believe the breach did not affect employees outside the department. …

Some lawmakers have announced they will investigate the breach. 'It is extremely concerning that the largest private provider of background investigations to the government was hacked,' said Rep. Elijah E. Cummings (Md.), the ranking Democrat on the House Oversight and Government Reform Committee. 'I am asking Chairman [Darrell] Issa to work with me in having our committee investigate this matter with the utmost urgency.' The USIS breach 'is very troubling news,' said Sen. Jon Tester (D-Mont.), a Homeland Security Committee member. 'Americans' personal information should always be secure, particularly when our national security is involved. An incident like this is simply unacceptable.'

The next day, many news outlets (including **Federal Times**) reported that both DHS and OPM suspended USIS' contract work. The Federal Times story stated—

The Department of Homeland Security has suspended background checks and most contracts with contractor USIS after a cyber attack may have accessed the personal information of DHS employees. … [The DHS spokesperson] said the agency has determined that some DHS personnel have had their personal information compromised and the agency has notified its entire workforce to monitor their financial accounts for suspicious activity. … DHS has also stopped providing sensitive information to USIS, according to a DHS official, which means that many of its contracts are in a state of suspension.

The financial results of being unable to perform contract work should be obvious. What may be less obvious, however, are the potential downstream effects for USIS associated with this situation. (See, for example, our discussions of data breaches at SAIC.) Suffice to say this situation has the potential to be catastrophic for the company.

Broken down to fundamentals, risk management consists of (1) identifying risks, (2) assessing those risks in terms of probability of occurrence and consequence, (3) establish mitigation strategies, (4) execute appropriate mitigation strategies at appropriate times, (5) monitor for inflection points. We cannot stress enough that government contractors need to consider the full panoply of risks associated with their program portfolios. We cannot stress enough that government contractors need to honestly evaluate both the probability of occurrence and the probable consequences of occurrence. We cannot stress enough that risk mitigation strategies need to be viewed as investments rather than as expenses.

There is a quantifiable ROI associated with cyber-security. But don't take our word for it: just ask the folks at USIS.