

# 10 Challenges Government Contractors Face with Security Information Management

by Joe Gottlieb

It is challenging to stay ahead of the growing types of *attacks* on business data/information. Security information management is even more daunting for contractors, serving the private and public sectors. Specific agreements made between the contracting agency and their clients impose requirements and penalties in case of a data breach. This drives even greater *accountability* for contracting firms.



Today, government contractors are finding themselves at the nexus of attacks and accountability... Why?

## HACTIVISTS

## LOGICAL ENTRY POINT

## ANY BREACH IS A BAD BREACH

## LACK OF CONTROL

## PROJECT PARTITIONING

## RISKY WORKFORCE

## NEGATIVE PERCEPTION

## UNDESIRABLE MISSIONS

## CONTROVERSY BREEDS ATTENTION

## DANGER IN DISCLOSURE

**1 Hactivists.** While some dismiss organizations like “Anonymous” as being nothing more than righteous graffiti artists, their focus to find chinks in the government’s data management armor is not without impact. Government contractors, like Lockheed Martin, have experienced major business disruption even though the attack on them did not yield any stolen data.

**2 A logical entry point.** Government contractors build business links between themselves and the agencies they serve. Shared systems and networks, and even funded personnel, are exploited to gain entry to federal agencies. As a trusted connection in the government supply chain, more diligence is required to secure access and activities taking place across those links.

**3 Any breach is a bad breach.** Even when no data was stolen, just accessing a network or system is perceived as a successful attack. Why? It achieves a level of damage that can’t be quantified: loss of public confidence, a drain on staff, and a distraction to the business that is difficult to recover from. Not to mention getting the attention of regulators and auditors who monitor controls for weaknesses.

**4 Lack of control.** Managing large projects as an outside vendor, particularly when your client is a government agency, is exponentially more complex than projects clients deal with directly. The data you need lives outside of your control, along with the people who are responsible for it, the processes that govern how it is distributed and retained.

**5 Project partitioning.** Government contractors must compartmentalize the information, people and processes from each agency, program and project—from the way data is managed, to the personnel associated with the project, and everything in between.

**6 A risky workforce.** Program cutbacks create budget pressure for government contractors who still have to deliver the goods, often with a small, temporary staff who may not be skilled or invested in maintaining best practices for controlling information. This group is seen as a target vulnerable to paid exploits.

**7 Negative perception.** Major scrutiny is placed on tax dollars, and government contractors are perceived to be opportunists on “the take.” That means any risk exposed will be exploited as evidence of agencies abusing taxpayer dollars and confidence.

**8 Undesirable missions.** Government contractors are often responsible for programs that even their clients would not take on...another reason they are highly targeted. Yet, in many cases, they are not “in the know” or have full visibility to all the pieces of the puzzle.

**9 Controversy breeds attention.** There is an even bigger appetite to target government contractors as they are often involved in highly sensitive or controversial programs. A “win” or takedown of an agency which could point to potentially unsavory activities is just more notoriety for the cybercriminal.

**10 Danger in disclosure.** Unlike private sector companies who are able to manage what, how, and when they disclose a breach to their shareholders, customers and markets, government contractors must operate under strict terms of their agreement and external agency controls, which often dictate how information breach disclosures must be handled. This can produce challenging scenarios in which the contractor must absorb all of the press and public scrutiny while not being able to seize control and manage all aspects of the aftermath.

With these challenges in mind, government contractors need to be systematic and comprehensive in their security information management practices. **Sensage Security Intelligence Solutions** enable proactive coordination—and convergence—of security processes with a single data architecture that scales to petabytes and beyond. Learn how organizations leverage Sensage to enhance their visibility into insider threats, APTs, next-generation malware, botnets and more, please **contact us for a demo.**

