We have not heretofore commented on the loss of the control codes for the International Space Station (ISS). You may already know that **somebody stole** an unencrypted NASA laptop and thus gained possession of the "algorithms" used to control the ISS. It occurred to more than one person that such an incident would be a great start to an action movie, perhaps starring Tom Cruise, George Clooney, or Matt Damon—but unfortunately it was all too real. Proving once again that life is stranger than Hollywood can dream up, NASA had to accept that some person or persons unknown was in possession of the codes used to control the ISS.

That particular incident is only one of the 48 NASA laptops or mobile devices stolen from the Space Agency between 2009 and 2011, according to Congressional testimony by the NASA Inspector General. According to the NASA IG, data lost in these thefts included "export-controlled, Personally Identifiable Information, and third-party intellectual property." Yet despite the ongoing risk posed by data loss, to date only one percent of NASA laptops and other mobile devices have been encrypted.

In this **PCWorld** article, the author explored some of the implications from unencrypted devices. He wrote—

Lost laptops and lost mobile phones have long topped the list as the biggest nightmare for security chiefs and PR teams (see this Laptop Losers Hall of Shame for some older cringe-worthy stories). Why does encryption continue to pose such a big business challenge?

NASA offers a good example. It doesn't have an agency-wide data encryption system or solution. Individuals can encrypt a laptop at the file, folder, or drive level , but that could leave too much room for error or leave too much up to user discretion. A centralized, managed encryption solution for your whole fleet of mobile devices is a better idea, but obviously may involve more costly enterprise resources. Implementing such a system across a chain of command, with lots of people and systems involved, no doubt requires a lot of planning and commitment.

Considering that the average value of an individual lost laptop has been computed as more than $49,000
, however, making sure each laptop is encrypted before it leaves the room with sensitive data on it is probably well worth the investment.

Readers of this blog already know about our position on this particular issue, thanks to Science Applications International Corporation (SAIC) and a stolen unencrypted laptop full of the personal information of 4.9 million TRICARE participants. Yes, you read that correctly:

SAIC lost the personal information of *4.9 million* TRICARE beneficiaries. As **we reported** —

So, let's see now. We were at about $36 million or so. Plus $4.9 billion in potential legal damages. Plus $147 million in credit monitoring services. Hey SAIC, might want to rein in those rogue employees of yours. You know, the ones who can't be bothered to encrypt their laptop hard drives?

That wasn't our only article about SAIC. We also **told you** about the company's problems with New York City. As we reported, SAIC faced troubling allegations regarding its "City Time" project, including receipt of kick-backs from a subcontractor and timekeeping irregularities by SAIC's project manager. Between the City Time and the TRICARE legal hassles, we figured that SAIC had a full plate of problems with which to deal.

Well, SAIC is back in the news, and we have some updates on those two stories to share with our readers.

On March 14, 2012, Bloomberg Businessweek **reported** that SAIC "agreed to pay $500.4 million under a deferred prosecution agreement to resolve claims that it conspired to defraud" New York City with respect to the City Time project. The article stated—

SAIC admitted it failed to investigate claims that a manager of the CityTime payroll project directed staffing tasks to a single subcontractor, Technodyne LLC, in exchange for kickbacks, according to documents unsealed today by federal prosecutors. The McLean, Virginia-based company also failed to notify the city of the claims …

The city was billed about $690 million for SAIC to create a now-operational Web-based, time-keeping payroll management system … Payments to Technodyne ballooned to $325 million from $17 million, even as the contract was amended to transfer cost overruns to the city, according to a statement of responsibility submitted by SAIC.

Bloomberg also reported that—

SAIC agreed to the filing of one count of conspiracy to commit wire fraud and agreed to disgorge proceeds of the offense, including $370.4 million in restitution to the city and a $130 million penalty, according to a Justice Department letter describing the settlement. An independent monitor will be appointed to ensure compliance with the accord and with procurement policies.

If SAIC pays the money and cooperates with federal investigators, the U.S. will seek to have

the charges dropped after three years, according to the agreement.

'Those responsible for directly managing the project failed to enforce the company's procurement policies in ways that allowed the irregular Technodyne relationship to continue,' according to the company's statement of responsibility. …

The project manager, Gerard Denault, was arrested in May and charged with fraud and conspiracy. His case is pending. … Prosecutors have charged 11 defendants plus Technodyne. One died, two pleaded guilty, and eight cases are pending ….

The bottom-line, as reported by Bloomberg is that "the $500 million [settlement] represents the '*largest by dollar amount arising out of any state or government contract fraud in history*'…."

Oh, but that's not all. Remember SAIC's stolen TRICARE laptop? Well, according to this **Nextgov story**, some of the TRICARE beneficiaries have "discovered bogus charges on their credit card statements and unauthorized bank transactions." The Nextgov article provided details, gleaned from one of the pending suits against SAIC, regarding the problems experienced by several people. The article reported—

The amended complaint said TRICARE beneficiaries had to take extensive steps to protect their financial information.

The plaintiffs 'had to cancel credit cards and close bank accounts; open new credit cards and bank accounts; stop direct deposits to those compromised accounts and re-enroll in direct deposits for new accounts; stop recurring electronic payments from compromised accounts and re-enroll in electronic payments through new accounts; and otherwise spend time and money in mitigation responding to notifications following the wrongful disclosure that certain financial accounts have been compromised,' the complaint said.

Dr. Deborah Peel, founder of the Patient Privacy Rights Advocacy Group in Austin, Texas, said unwanted marketing, credit card cancellation, and identity theft are typical and expected when sensitive, richly detailed personal health data is breached. It could take years to discover the repercussions of stolen medical information, she said.

Interestingly, the story also noted that the amended complaint alleged that the theft of the TRICARE data may not have been a random act. Nextgov reported—

The new complaint alleges that the theft was targeted. The SAIC employee's car, a 2003 Honda Civic, was parked in a garage that housed many luxury cars, 'yet the thief or thieves,

who went to great effort to avoid security, did not break into any of the luxury cars in the garage, targeting instead the relatively inexpensive car containing the confidential data.'

The complaint added, 'The thief or thieves stealthily broke into the employee's Honda Civic and took the unencrypted backup tapes and records, thereby gaining information worth billions of dollars. The nature of this theft supports the logical inference that the thief or thieves were specifically targeting the confidential information contained on the backup tapes and records.'

The Nextgov story also noted that SAIC is currently facing eight separate lawsuits related to the data loss.

How much more can we add to the facts of the two stories? We here at Apogee Consulting, Inc. frequently urge our readers to invest in their internal controls, calling it cheap when compared to the full cost of non-compliance. How much clearer can the math be? In SAIC's case, one single state/local project led to a $500 million settlement, and one single failure to secure client data has led to eight separate lawsuits and a potential legal liability of *more than $5 billion* .
How much more can one corporation, no matter how large, afford? At what point does the Board of Directors—or the shareholders—start to lose confidence in the executive leadership team?

Remember, SAIC only recently became a publicly traded company. From its founding in 1969 through 2005, it was an employee-owned company. By its **own description** —

… SAIC had become a company of entrepreneurs. 'Not just one or two at the top,' says [Founder Bob] Beyster. 'A company in which those who are motivated and capable can organize, manage, and assume the risk of different aspects of the company. In return they received not only salary, but ownership of the company.'

The thing is, the SAIC of today isn't the SAIC of 1969 or even 1999. It's a publicly traded company with responsibilities to its shareholders. We wonder if perhaps it's time, or even past time, for the company to consider changing its entrepreneurial culture and move toward a more centralized command-and-control structure—one that might act to mitigate some of the corporate risks that do not seem to be fully managed by its employees.