

At the airport

Avoiding laptop separation anxiety

JOHN GLENN, MBCI

Enterprise Risk Management practitioner

Dell, the computer company, released a study in June 2008 titled "*Airport Insecurity: The Case of Lost Laptops.*" The study was conducted by Ponemon Institute LLC for Dell. (http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf)

The study is telling in many respects, especially in the number of notebook computers that "go missing" and the lack of security in place on these machines. It's also interesting to note which airports have the highest - and lowest - numbers of missing computers. LAX leads the list with 1200 units "lost" in a week, closely followed by MIA with 1000; DCA and IAD are close to the bottom in their airport class.

The study, as expected had a number of recommendations.

Recommendations and Conclusion

Lost laptops in airports are a serious issue for business travelers and their companies. As revealed in this study, very often business travelers' laptops contain sensitive or confidential business information that is vulnerable to a data breach.

According to our *Cost of Data Breach Study*, the average business cost when confidential personal information is lost or stolen is **\$197 per record**.(U.S. Cost of Data Breach Study, Ponemon Institute LLC, November 2007) Obviously, even one missing laptop can become a serious problem for any organization. To avoid having this occur, we recommend the following simple steps.

- ✓ Label your laptop. Provide your full contact information so that if the device is found, airport personnel will be able to reach you or your company quickly.
- ✓ Allow enough time. Airline travel is a hassle that only gets worse when you don't allow enough time. Stupid mistakes can be avoided if you slow down your pace.
- ✓ Carry less and think ahead. Have a mental strategy when removing laptops and other possessions prior to screening at a security checkpoint.
- ✓ Take appropriate security measures to protect your information. Consider the use of encryption technologies and always backup your system.
- ✓ Think twice about the information you carry on your laptop. Is it really necessary to have so much information accessible on your computer?
- ✓ Know who to call. Airports need to do a better job coordinating the lost and found process, especially when it concerns the loss of a laptop computer or other data-bearing devices.

Most of the recommendations really fall into the category of "just common sense."

Hurry up and wait

"**Allow enough time**" is, to me, a no brainer. I understand that *sometimes* an urgent flight is required, but having been in business for more than a couple of years, I know that - conservatively - 85% of all flights can be booked well in advance (saving the organization substantial money) and that early arrival at the airport does not mean reduction in productivity.

The study reports that 70 percent of those interviewed claimed to feel rushed at the airport. A lot of that "rushed" feeling is waiting to get a boarding pass and to clear security. Most boarding passes can be printed by or for the travel before heading for the airport.

If the Busy Executive hangs around the office or home using the computer, the same Busy Executive can use a laptop computer at the airport; most airports now have free or fee Wi-Fi, so even connectivity is possible.

In other words, the only time Busy Executive will suffer keyboard separation is during the security check.

Forbes Traveler has a 10-slide presentation that may help travelers get through the security check a little faster. (<http://www.forbestraveler.com/jets-planes/speed-through-airport-security-story.html>)

Unfortunately, the "Clear" TSA Registered Traveler program operated by Verified Identity Pass and mentioned in the Forbes' presentation shut down in June 2009 for, according to an Associated Press (AP) article, lack of funding. (<http://www2.tbo.com/content/2009/jun/23/fast-lane-airport-security-service-shuts-down-leav/life-travel/>)

Two other companies, Vigilant and FLO, offer similar service, but they are far smaller, according to the AP.

Use protection

Another no brainer is "**Take appropriate security measures to protect your information.**"

According to the survey, 65 percent of the respondents claimed that they, or their organizations "Do not take steps to protect the confidential or sensitive information contained on laptop when traveling on business."

No system password protection.

No media encryption.

No file passwords.

No backups.

Granted, biometric security may be a bit much for most computers, but to go completely naked into the night as it were never will make a *Best Business Practice* list.

At the most basic level, there should be a strong password at the system level, sensitive files (including emails) need to be individually password protected, and critical data needs to be backed up.

If Busy Executive intends to use the airport - and now some airline - Wi-Fi, data encryption needs to be in place so all those bits and bytes traveling across the ether are scrambled.

Consolidate to expedite

Travelers can help prevent the computer from being accidentally - or not - picked up by someone else at the end of the scan tunnel by following the "**Carry less and think ahead**" admonition.

Empty pockets and collect all loose items - change, keys, cell phones, etc. - and stow them in a bag to be scanned. Untie shoe laces and loosen them; better yet, wear loafers/slip ons. For quick retrieval, stick ticket/boarding pass and picture ID into a shirt pocket (never a hip pocket) or a special hang-around-the-neck ID/Passport/Boarding Pass holder made for just this exercise.

Rodeo champion-size belt buckles and the belt should be removed and passed through the scanner.

The idea is to have everything ready when the traveler and computer are separated so that the traveler will be on the other side of the scanner when it spits out the computer.



Travel Bag from <http://www.travelonbags.com/pages/XXXXX/200/249.html>

Must the data be on the machine?

Another recommendation: "**Think twice about the information you carry on your laptop**" has me nodding my head in agreement.

When I worked for a transportation company, I recommended scanning contracts to CD. One of the brighter managers suggested that it would be convenient if he could have a copy of the CD for his trips to client sites; that way, he said, he could update the contract on the spot, print out the relevant pages, and get signatures while the customer was sitting across the table.

It seems to me it would be easy to comply with the study recommendation AND have all the information the traveler may need if the traveler took the manager's approach: put information on a CD (make a second back-up, and **then** delete the file[s] from the computer).

Avoiding laptop separation anxiety

Put the CD in carry-on or stowed luggage; anyplace but with the computer. If the computer goes astray, the CD still may be available. There is an excellent probability that the customer will have a computer that can read the CD and business will go on.

Think about this one

The one recommendation to which I take limited exception is "**Label your laptop.**"

Yes, label it, but do **not**, as the recommendation suggests, "Provide your full contact information." The only information that ought to be on the label is a set of telephone numbers - the owner's cell (since the owner still may be at the airport) and the owner's office (in the event the owner is airborne). If there was a way to put a temporary, easily removable tag on the machine, I would suggest putting flight information on the tag - airline and flight number.

The owner's name might be OK unless the owner is a "known" in his or her field, but never, never, never include the owner's organization. Imagine a modern Mata Hari labeling her computer "*Property of Spies-R-Us*" or "*If lost, call Spies-R-Us at 8**-Spy-4You.*" Our Busy Executive may as well put the machine password - if there is one - on a Post-It (™) and stick it on the keyboard touchpad.

Put the two phone numbers (ibid.) on an at least semi-permanent tag located in a fairly prominent part of the machine.



Mata Hari pictures at http://images.google.com/images?hl=en&q=Mata+Hari&um=1&ie=UTF-8&ei=_gp7SoasH4aHtgfk7-j3AQ&sa=X&oi=image_result_group&ct=title&resnum=4