Hal Berghel

STUCK ON STUPID: IT'S DUMBEST DECISIONS

As I write this, The BP Gulf oil spill remains the top news story. By way of background, this environmental nightmare began when the exploratory drilling rig, Deepwater Horizon, operated by Transocean, Ltd, under lease to BP caught on fire April 21, 2010 resulting in the death of eleven Transocean employees and injury to seventeen more. The fire could not be extinguished, which culminated in the total destruction and sinking of the rig, and ultimately the breaking of the pipe connecting it to the seabed. As in all wells of this type, a blowout preventer had been installed. But the blowout preventer didn't work. A well cap was placed over the defective blowout preventer, but it didn't work either. A "junk shot" of golf balls and ground up tires was shot into the well to clog the blowout preventer, but that didn't work. At this writing, BP has just placed a lower marine riser package (LMRP) containment cap over the defective blowout preventer and is capturing 16,000 barrels per day of oil and 22 million cubic feet of natural gas. Unfortunately, the production of well MC252 still far exceeds the recovered volume, so thousands of barrels of oil continue to spill in the gulf as you can see from the photo on the next page. Thus began one of the greatest environmental disasters in United States history.

Why did this happen? The BP MC252 environmental disaster was a product of cascading bad decisions. By the time you read this column, the full account may be available. But even at this early stage, several stupid mistakes can be identified - mistakes by the drilling contractor, BP, the federal inspectors who approved the project - there's enough blame to easily cover all participants. From the point of view of an outsider, the mistakes can all be subsumed under the rubric of an absence of a backup plan in case something went wrong! The blame lies with the people who approved MC252 - the paradigm case; it seems, of a mistake waiting to happen. What were these decision makers thinking?

MC252 will join the Kansas City Hyatt Regency walkway collapse, the Ford Pinto gas tank defect, the Union Carbide Bhopal disaster, to name but a few, as poster children for "industrial strength dumb mistakes."

We in IT are not immune. In the remaining pages I'll illustrate a few of our most recent debacles: each a product of unrefined intellect unleashed on mundane activities.

I DON'T CARE IF THE DOCUMENTS ARE MARKED "TOP SECRET," MAKE ME A COPY

It is easy to come up with a list of technology "bad ideas." The IBM PC jr, Control Data's 10-bit byte, Windows Millennium Edition, the IEEE 802.11 implementation of the RC4 algorithm in WEP, - you get the idea. Just look at a few dozen websites and you can see that the web doubles as a toxic waste site for digital multi-mediocrity. Bad ideas will always outnumber the good.

But some brain spasms just call out for more than honorable mention. They stand out as triumphs of the will in confusing what we can do vs. what is really worth doing - a failure to understand the essence of the effort. My first example is the cavalier attitude IT professionals, managers and executives have with the practice of photocopying.

In the Jurassic period of copiers, say 1970-1990, there was a 1:1 relationship between the scanning of the image and the printing of the copy. Those of us who are long enough in the tooth may remember patiently waiting for copies while the little light leak under the document cover went from left-to-right as each copy was printed. The reason for that was that there was no way to store the image, so the source document had to be re-scanned over and over and over. Hold that thought.

For the past decade, give or take a few years, the telltale moving light leak vanished for mainstream business copiers. Hmmm. What could that mean? There aren't too many options when you think about it: the scan engine is no longer directly coupled with the print engine. That's pretty obvious. So the original scanned image must be stored somewhere. So the operative question becomes, what happens to the copies on the stored media once the copies are completed?

There isn't a competent IT professional out there that doesn't understand the phenomena of re-allocation of file space. We have known for decades that deleting files in Windows doesn't delete the files at all - it just links the file to the Recycle Bin. And emptying the Windows Recycle Bin doesn't delete files either, it just re-allocates the file space to the file manager for subsequent reuse.

Let's return to our held thought. If only one scan of a document can provide a limitless number of photocopies, the print engine must be driven by data storage - e.g., hard disk. So is it reasonable for anyone to think that the mini-operating system in the photocopier is sanitizing the used file space. Windows doesn't do this. Is it really reasonable to expect the mini OS in a copier to do it?

Enter the latest craze in identity theft: harvesting sensitive data from photocopier hard drives. That this is happening is not news - criminals have been doing this for years. What is news is

Oil Leak from MC252 from the Skandi ROV2 Spill Cam -after the June 3, 2010 LMRP repair

that so many IT professionals, managers, and executives seem to remain clueless about the vulnerability.

Witness the February, 2010 CBS News report (text and video at http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml) on the practice of harvesting data on de-commissioned photocopier hard drives. The reporter bought four used photocopiers from a warehouse in New Jersey and contracted with a security firm to retrieve the photocopy data. Two photocopiers had enjoyed an earlier life in the Buffalo, N.Y. Police Department - one in the Sex Crimes Division and one in the Narcotics Unit. Take a guess at what information was recovered from those hard drives. The Buffalo Police Department let the copiers out the door without having the disks sanitized. This is not rocket science. One has to ask "What was the IT manager thinking?" "Who wrote their INFOSEC policies?"

Another copier came from the Affinity Health Plan. Take a guess what information was on that drive?

Software tools for recovering digital data on hard drives have been widely available for more than thirty years beginning with Norton Utilities for CP/M and DOS. Modern refinements include the Forensics Toolkit, X-Ways Forensics, and Encase. For those interested in the fine art of disk sanitization, see http://www.berghel.net/col-edit/digital_village/aug-06/dv_8-06.php. How is it that this didn't trigger an alarm with IT folks years ago?

What is more, photocopier disk drives can be sanitized just like any other storage device. So how is it that IT managers didn't insist on either a disk sanitization or disk destruction protocol before copiers were de-commissioned. Manufacturers provide such software, and 3rd party software can be used if the drive is removed from the photocopier. IT folks should have known better. This is the digital equivalent of the BP oil spell. What were they thinking?

Dumb Down The Redacted Data

The next example comes from the archives of our own modern-day Cerberus, the Transportation Security Administration (TSA).

TSA released a redacted copy of their May 1, 2008 screening procedures manual document. To no one's surprise, the document made its way to cyberspace. So far, so good. Redaction has been widely used by the government for Freedom of Information Act (FOIA) compliance since the 1960's.

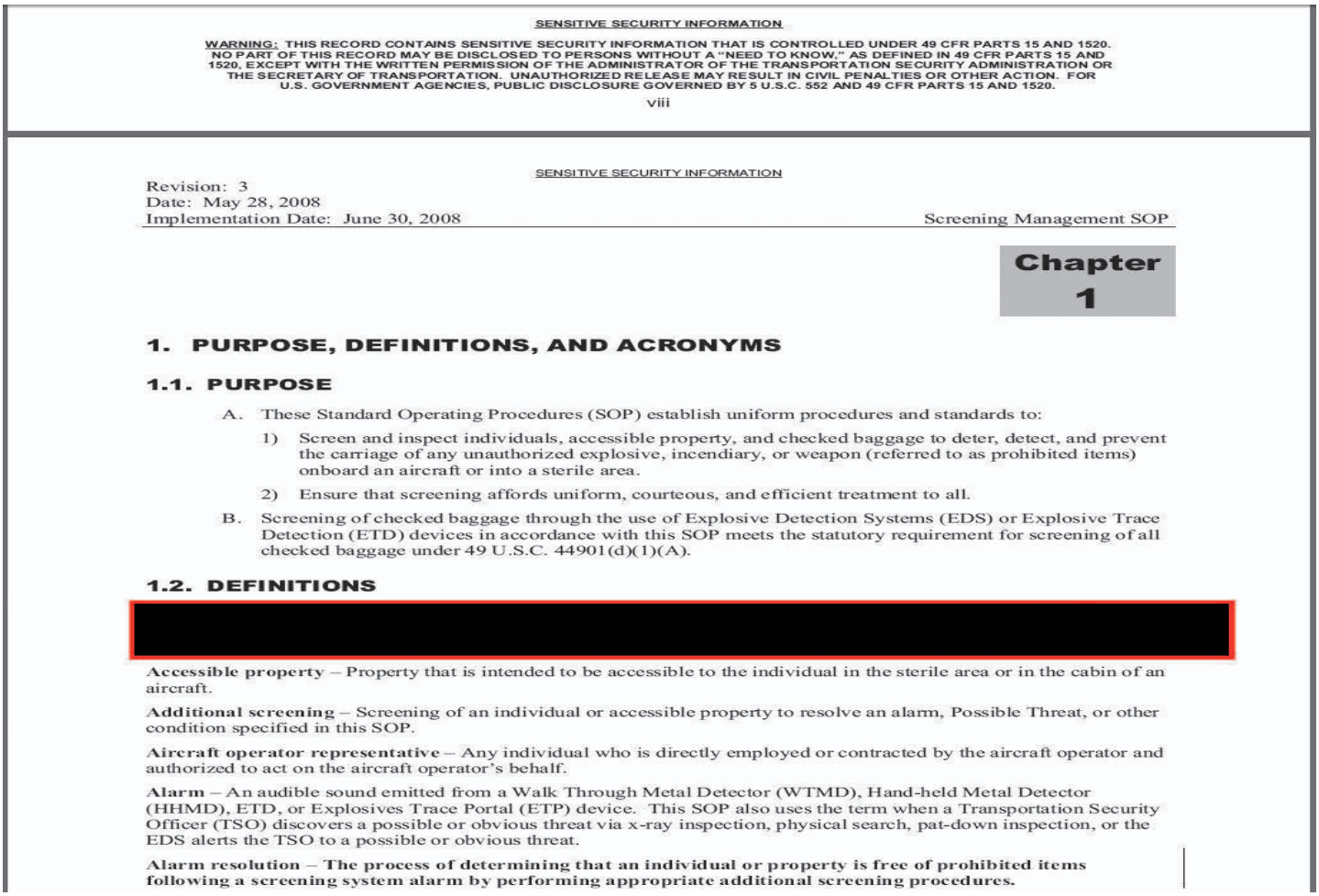
FOIA in its various amended forms attempts to balance the public's right to know with the need for secrecy relating to national defense, matters that could destabilize financial institutions, internal policies of federal agencies, information relating to ongoing prosecution, and so forth. The "compromise" often involves redaction - i.e., the technique of removing sensitive information so that the spirit of the document may be understood, but not the detail covered by the exemptions.

Ok, so redaction is 40+ years old and well-understood. What's this got to do with TSA? Well, although many of us have come to know and understand redaction, it's still an infant art form when it comes to some TSA supervisors. They chose to do the redaction digitally by imposing an opaque layer over a textual layer in a PDF document. To quote the source of the disclosure, WikiLeaks:

> "To redact the TSA document for public release, officials apparently used a computer program to blacken particularly sensitive parts of the handbook, including which types of travelers are exempt from various kinds of random and required screening, the procedure for CIA officers escorting foreign dignitaries and others through checkpoints, the minimum gauge of wire used to calibrate X-ray machines, and the types of chemicals used for cleaning explosive residue scanners.
>
> The document was then published online as a PDF, a common file format used widely by the government. To redact it, officials' obscured text using a program which successfully obscures the text as viewed on a computer monitor. But the information wasn't deleted. Highlighting the text of the PDF page and then using the copy and paste functions on a computer easily revealed the hidden information." (http://wikileaks.org/wiki/TSA_to_Conduct_Full_Review_After_Leak_of_Sensitive_Information)

The next two images illustrate the point. Image 1 is a page from the redacted manual.

Redacted page from 2008 TSA Screening Management Procedures manual posted as a PDF file with black redaction layer added in PDF



SENSITIVE SECURITY INFORMATION

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 CFR PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 CFR PARTS 15 AND 1520.

viii

SENSITIVE SECURITY INFORMATION

Revision: 3
Date: May 28, 2008
Implementation Date: June 30, 2008 Screening Management SOP

Chapter 1

1. PURPOSE, DEFINITIONS, AND ACRONYMS

1.1. PURPOSE

A. These Standard Operating Procedures (SOP) establish uniform procedures and standards to:

1) Screen and inspect individuals, accessible property, and checked baggage to deter, detect, and prevent the carriage of any unauthorized explosive, incendiary, or weapon (referred to as prohibited items) onboard an aircraft or into a sterile area.

2) Ensure that screening affords uniform, courteous, and efficient treatment to all.

B. Screening of checked baggage through the use of Explosive Detection Systems (EDS) or Explosive Trace Detection (ETD) devices in accordance with this SOP meets the statutory requirement for screening of all checked baggage under 49 U.S.C. 44901(d)(1)(A).

1.2. DEFINITIONS

[redacted]

Accessible property – Property that is intended to be accessible to the individual in the sterile area or in the cabin of an aircraft.

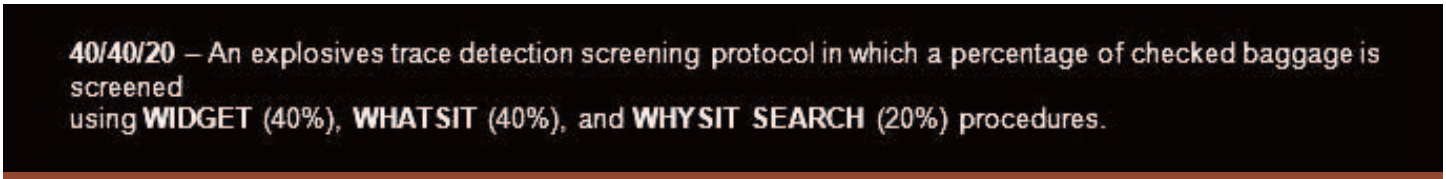
Additional screening – Screening of an individual or accessible property to resolve an alarm, Possible Threat, or other condition specified in this SOP.

Aircraft operator representative – Any individual who is directly employed or contracted by the aircraft operator and authorized to act on the aircraft operator's behalf.

Alarm – An audible sound emitted from a Walk Through Metal Detector (WTMD), Hand-held Metal Detector (HHMD), ETD, or Explosives Trace Portal (ETP) device. This SOP also uses the term when a Transportation Security Officer (TSO) discovers a possible or obvious threat via x-ray inspection, physical search, pat-down inspection, or the EDS alerts the TSO to a possible or obvious threat.

Alarm resolution – The process of determining that an individual or property is free of prohibited items following a screening system alarm by performing appropriate additional screening procedures.

A simple cut-copy-paste operation on the redacted area looks like this when pasted into Microsoft Word:



40/40/20 – An explosives trace detection screening protocol in which a percentage of checked baggage is screened
using **WIDGET** (40%), **WHATSIT** (40%), and **WHYSIT SEARCH** (20%) procedures.

The Redacted Area in Image 2 Un-redacted (with author's redaction added for the benefit of the G&L lawyers)

What on earth were these TSA IT folks thinking? Shouldn't the public be made aware of the position description for the job these supervisors filled? What did the operative INFOSEC policies look like? We have yet another example of dumb-on-demand.

By the time that the TSA removed the posted document on December 7, 2009, the proverbial toothpaste was well out of the tube - cf. the WikiLeaks.org posting at http://wikileaks.org/wiki/US_Transportation_Security_Administration:_Screening_Procedures_Standard_Operating_Procedures,_1_May_2008).

Conclusion

It's not unusual for smart people to have really bad ideas: look no further than Edison's intransigence to distribute electricity to municipalities with direct current. Unlike Tesla, Edison just didn't get it. For a visual paradigm of dumb-on-demand, check out the attempt to recycle a dead, beached whale with dynamite (http://www.youtube.com/watch?v=ZFwxH3PPWiU). But fortunately for us, most of our IT blunders are neither life-threatening nor environmentally hostile.

Hal Berghel is Director of both the UNLV School of Informatics and the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). His consultancy, Berghel.Net, provides security and management services to government and industry.