Noted Science Fiction author **Charles Stross** stole our title for today’s article: **The Atrocity Archives**. Okay, he didn’t steal it, but it would have been *perfect* for the following potpourri of mini-articles. Oh, well.

1.

The Boeing Company recently **agreed** to settle a “defective pricing” civil suit “alleging that the company unlawfully inflated the price it charged the Air Force to manufacture the Towed Decoy System for the B-1 bomber.” The Government alleged that “Boeing failed to disclose to Air Force contract negotiators that it had previously manufactured TDS kits for much lower costs, largely by outsourcing much of the work to outside vendors and subcontractors.” The case was dismissed without any admission of wrongdoing by Boeing.

1.

We certainly don’t want to be seen as being overly alarmist. So, we’re just saying that the so-called “Iranian Cyber-Army” “may have successfully infected as many as 20 million PCs.” Our cyber-security stories don’t interest many site visitors for some strange reason, but here’s **a link** to the story at computerworld.com. Again, there’s no reason to be overly concerned about this group, which may or may not be connected to the Iranian government, but which is known for having hacked both Twitter and Baidu. Don’t be worried about its for-rent botnet service. Ignore the fact that investigators found “an administration interface where people who want to rent the botnet can describe the machines they would like to infect and upload their own malware for distribution by the botnet.” According to one source quoted in the story, “ ’you provide the number of machines and their region. You then provide the malware download URL, and they will do the malware installation for you.’" Nope. Nothing to see here. Move along, please.

1.

And while you're not looking at your lack of cyber-security, take no notice of Darnell Albert-El, of Richmond, Virginia, who was **sentenced** to serve 27 months in prison for " hackin g into his former employer's website" and "one count of intentionally damaging a protected computer without authorization." Albert-El, a former IT Director for Transmarx, LLC, was fired by his employer. After his termination, "he used a personal computer and an administrator account and password to access the computer hosting the Transmarx website." What did he do with his unauthorized access? He "caused the transmission of a series of commands that intentionally caused damage without authorization to the computer by deleting approximately 1,000 files related to the Transmarx website." What was his motivation? According to the DOJ, "Albert-El admitted that he caused the damage because he was angry about being fired." Note to self: When firing your IT director, make sure to disable his/her account access and passwords.

1.

Former Contracting Officer and Army Major Roderick Sanchez **pleaded guilty** to one count of bribery "
for accepting money and items of value in return for being influenced in the awarding of Army contracts." According to the DOJ, "Sanchez admitted that … he accepted illicit bribe payments from foreign companies seeking to secure Army contracts. In return, Sanchez used his official position to steer Army contracts to these companies. During the course of this criminal scheme, Sanchez accepted Rolex watches, cash payments and other things of value totaling more than $200,000."

1.

Would you pay $6.50 per minute for video conferencing? Even if the phone bill ended-up being $55 million over a few months? Apparently, the Federal Communications Commission **would** . It wasn't the pricing that led to trouble for Viable Communications, Inc., it was the conspiracy to commit mail fraud. Let's let

the DOJ tell the story—

Beginning in approximately fall 2007, they conspired with others to pay individuals to make fraudulent VRS phone calls using Viable’s [Video Relay Service] VRS service. … John and Joseph Yeh paid Mowl and Tropp, who then would pay others to make the fraudulent phone calls using Viable’s VRS service. Viable then submitted the fraudulent call minutes to the FCC and was paid approximately $390 per hour for all VRS calls that Viable processed. … VRS is an online video translation service that allows people with hearing disabilities to communicate with hearing individuals through the use of interpreters and Web cameras. A person with a hearing disability who wants to communicate with a hearing person can do so by contacting a VRS provider through an audio and video Internet connection. The VRS provider, in turn, employs a video interpreter to view and interpret the hearing disabled person’s signed conversation and relay the signed conversation orally to a hearing person. VRS is funded by fees assessed by telecommunications providers to telephone customers, and is provided at no cost to the VRS user. … In addition to the indictment charging the Yehs, Mowl, Tropp and Viable, five other indictments were unsealed … charging an additional 22 people with engaging in a scheme to steal millions of dollars from the FCC’s VRS program. The indictments charge owners and employees of the following six companies with engaging in a scheme to defraud the FCC’s VRS program:

-

Viable Communications Inc. of Rockville, Md.;

-

Master Communications LLC of Las Vegas;

-

KL Communications LLC of Phoenix;

-

Mascom LLC of Austin, Texas;

-

Deaf and Hard-of-Hearing Interpreting Services Inc. (DHIS) of New York and New Jersey;

-

Innovative Communication Services for the Deaf Corp. (ICSD) of Miami Lakes, Fla.; and

-

Deaf Studio 29 of Huntington Beach, Calif.

Well, that’s the news for today. As we said, even though we could call this The Atrocity Archives, that title has already been taken. In any case, that was a work of fiction and these newlets are not fiction. We don’t make this stuff up.