Femtosecond®
www.femto-second.com

In the News

Volume 3 Issue 7

March 28, 2010

Economic News

Readers may recall from the last newsletter, the Park Avenue Bank in New York was shuttered. Now it seems the former president of this bank was charged with fraud (Federal Deposit Insurance Corp.), making false statements on a TARP application, mail fraud, bank fraud, bank bribery, making a counterfeit certificate of deposit, wire fraud and embezzlement [1]. Moreover, the Federal government named nearly 30 bankers from a dozen of the largest banks as co-conspirators in pricing of certain municipal derivatives [2]. In a further sign of financial trouble, regulators shut down GunnAllen Financial Inc., a Tampa-based broker-dealer leaving 400 financial advisors unemployed [3]. Meanwhile, new home sales fell for the 2.2% in February to a record low [4]. In another troubling sign of things to come, Social Security payouts will exceed revenue this year [5].

Moody's warned, the U.S. could lose its AAA credit rating if the current economic trends continue [6]. To illustrate the consequences, Fitch Ratings lowered Portugal's credit rating to AA- because of its soaring deficit [7]. The immediate impact was fear of a growing fiscal crisis in Europe [8]. Perhaps this is the reason demand for U.S. treasuries are weak [9]. Meanwhile, former Fed Chairman, Alan Greenspan, said the Federal regulators became complacent and failed during the financial crisis [10]. What's more, the current Fed chairman, Ben S. Bernanke, said bailout of large financial institutions must stop [11]. Elsewhere, the World Bank is predicting China's growth will be 9.5% for the year [12]. On the jobs front, for the week ending March 13, the first time unemployment claims fell to 457,000 [13]. For the week ending March 20, the number of first time jobless claims fell to 442,000 [14].

Until banks start lending money again to small business, economic recovery will be a lengthy process. For this reason, it's important for regulators to restore the health of the banking industry as soon as possible; while hoping there are no additional surprises along the way such as another large bank failure. March 19 was a busy day with seven financial institutions were shuttered: 31) American National Bank in Parma, Ohio; 32) Century security Bank in Duluth, Georgia; 33) Advanta Bank Corp in Draper, Utah; 34) Appalachian Community Bank in Ellijay, Georgia; 35) Bank of Hiawassee in Hiawassee, Georgia; 36) First Lowndes Bank in Fort Deposit, Alabama; and 37) State Bank of Aurora in Aurora, Minnesota [16]. Of particular concern was there was no buyer for the largest bank, Advanta which had had an estimated $247,000 in uninsured deposits [15]. What

(Continued on page 2)

IT Security

There is a growing concern for the safety of electronics used in automobiles. For example, in Texas, a hacker was able to disable over 100 cars using a wireless connection; the cars were equipped with a dealer installed black box designed to make repossessions easier [1]. In other news, researchers have discovered a new zero-date security bug in Microsoft's virtualization program that could allow hackers to bypass security and execute code [2].

Meanwhile China's demand that Google allow state sponsored monitoring has reached the point where the Chinese Government is advising business partners to look for Google alternatives [3]. What's more, there are concerns that when China penetrated the networks of American companies, including Google, they planted as yet undetected malicious software [4]. One estimate is that U.S. businesses lost $67.2 billion in 2005 due to cyber attacks [5].

Sometimes, information is best maintained in encrypted format. Case in point, personal information on 3.3 million student loan applicants was stolen [6]. The information stolen included social security numbers, dates of birth, and

(Continued on page 2)

Inside this issue:

Special points of interest:

- Chinese researchers publish how to shut down the U.S. power grid
- Hacker remotely disables 100 cars
- 41st bank closed
- Personal data on 3.3 million student loan applicants stolen

Economic News

(Continued from page 1)

that means is a small number of deposits were likely lost. Then on March 26, regulators closed the following four financial institutions: 38) McIntosh Commercial Bank in Georgia; 39) Key West Bank in Florida; 40) Unity National Bank in Georgia; and 41) Desert Hills Bank in Arizona [17].

1. Bray, Chad, Wall Street Journal, *Ex-Pres of Small-Business Bank Charged With Fraud*, March 15, 2010.
2. Humer, Caroline, Reuters, *Bankers named as suspected conspirators in muni case*, March 26, 2010.
3. Hielscher, John, Sarasota Herald-Tribune, *Regulator shuts down broker with Sarasota office*, March 24, 2010.
4. Bartash, Jeffry, Market Watch, *Sales of new homes fall to 308,000 annual rate in February*, March 24, 2010.
5. Walsh, Mary William, New York Times, *Social Security Payouts to Exceed Revenue This Year*, March 24, 2010.
6. Brown, Matthew, Bloomberg, *U.S., U.K. Move Closer to Losing Rating, Moody's Says*, March 15, 2010.
7. Brown, Matthew, Bloomberg, *Portugal's Debt Rating Lowered by Fitch on Finances*, March 24, 2010.
8. Rooney, Ben, CNN Money, *Stocks slip on Portugal credit woes*, March 24, 2010.
9. Lauricella, Tom, Wall Street Journal, *Debt Fears Send Rates Up*, March 26, 2010.
10. Matthews, Steve, Bloomberg, *Greenspan Says Fed, Regulators 'Failed' During Financial Crisis*, March 19, 2010.
11. Matthews, Steve, and Mattingly, Phil, Business week, *Bernanke Says Large Bank Bailouts 'Unconscionable,' Must End*, March 21, 2010.
12. Dyer, Geoff, Financial Times, *World Bank raises China growth forecast*, March 17, 2010.
13. Homan, Timothy R., Business Week, *Leading Economic Index in U.S. Rose 0.1% in February*, March 18, 2010.
14. Bartash, Jeffry, Market Watch, *Jobless claims fall by 14,000 to 442,000*, March 25, 2010.
15. Daly, Corbett B., Reuters, *U.S. FDIC shuts down 7 banks, 2010 total now 37*, March 19, 2010.
16. Fitzpatrick, Dan, Wall Street Journal, *Utah, Georgia Banks Closed*, March 20, 2010.
17. Lazarus, Anthony, Market Watch, *Phoenix's Desert Hills Bank closed in 41st failure*, March 26, 2010.

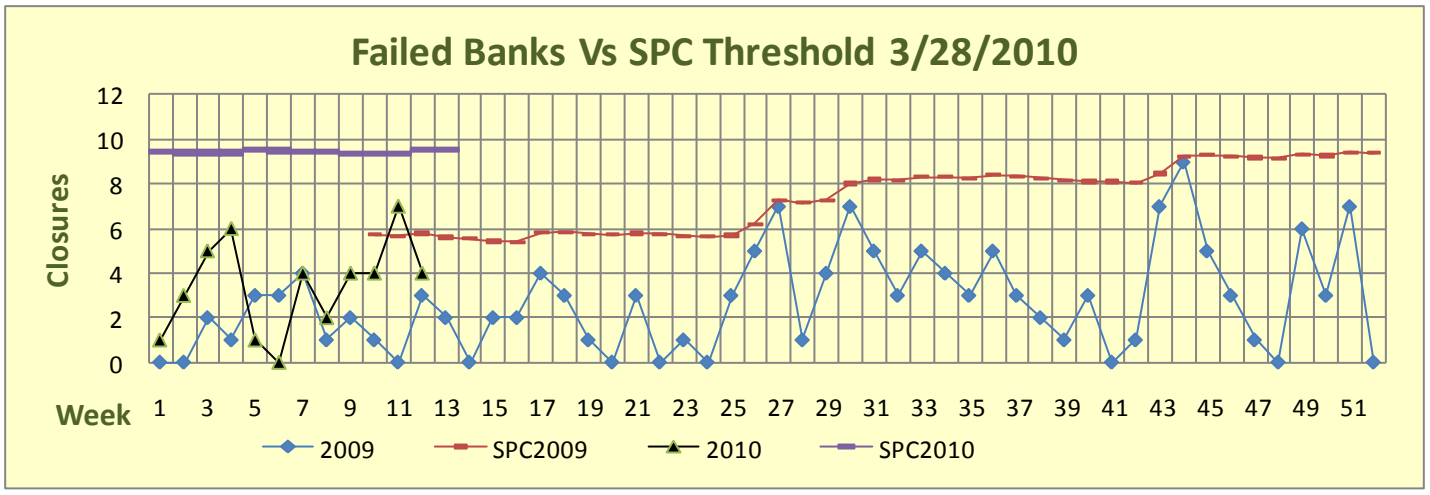
Where's the beef?–Clara Peller

IT Security

(Continued from page 1)

names [7].

1. Poulsen, Kevin, Wired, Hacker Disables More Than 100 Cars Remotely, March 17, 2010.
2. Moscaritolo, Angela, SC Magazine, *Security firm finds bug in Microsoft virtual program*, March 17, 201 0.
3. Shankland, Stephen, Cnet News, *China warns Google partners: Look for backup*, March 15, 2010.
4. Gertz, Bill, Washington Times, *Cyber-attack on U.S. firms, Google traced to Chinese*, March 24, 2010.
5. Bain, Ben, Federal Computer Week, *Senate bill targets countries where cyber-attacks against U.S. interests originate*, March 24, 2010.
6. Weil, Martin, Washington Post, *Data stolen from firm that handles student loans in Virginia*, March 27, 2010.
7. Karnowski, Steve, AP, *Student loan company: Data on 3.3M people stolen*, March 27, 2010.



Target US Power Grid

In past newsletters, we have described vulnerabilities with critical infrastructure systems that use the Supervisory Control and Data Acquisition (SCADA) protocol. Now researchers in China have published a paper on how to attack a small U.S. power grid and cause a cascading failure of the entire U.S. grid [1]. How long will it be before we suffer a serious attack against our power grid?

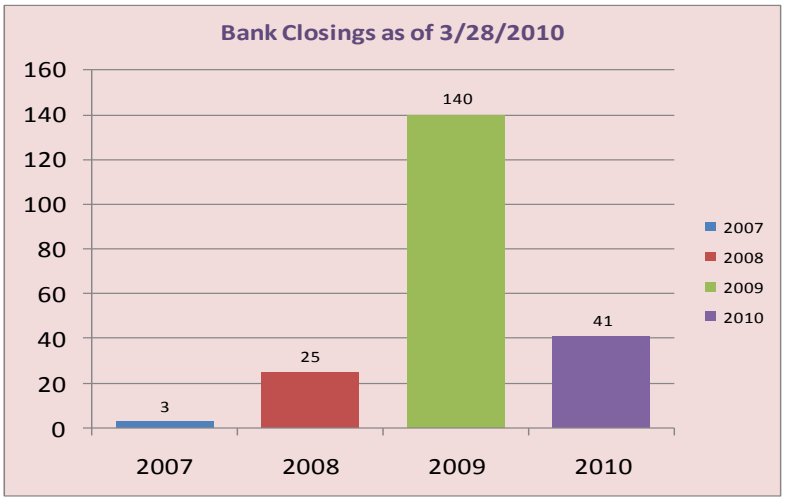
Another article suggests the number 1 doomsday scenario is a SCADA attack resulting in a power grid shutdown [2]. Furthermore, the source of SCADA attacks are difficult to trace and new smart grid technology are creating new cyber security concerns [3]. The main problem with SCADA is it was designed for isolated networks and security was not an original design consideration [4]..

1. Markoff, John, and Barboza, David, New York Times, *Academic Paper in China Sets Off Alarms in U.S.*, March 20, 2010.
2. Tynan, Tim, PC World, Five Doomsday Scenarios for IT: Tech Apocalypse, March 15, 2010.
3. Hubbard, Zachary, The Tribune-Democrat (Johnstown, PA), *Electricity disruptions a growing threat*, March 19, 2010.
4. Gaspard, Francois, and Hubrecht, Alain, Journal of Energy Security, *Tackling Critical Energy Infrastructure Network Interdependencies*, March 23, 2010.

Age wrinkles the body.

Quitting wrinkles the soul–

Douglas MacArthur



World News

While much has been said about China's currency manipulation, history shows this is an effective way to transfer wealth. For example, this technique was used by Japan to prosper at the expense of the U.S. [1]. In the case of China, the World Bank is predicting a growth of 9.5% for the year [2]. Meanwhile, the U.S. has acknowledged the problem and let China know it [3]. One report is estimating that China's unfair trade policies have cost the U.S. 2.4 million jobs between 2001 and 2008 [4]. What's more, China announced it plans to maintain the value of the Yuan thereby ensuring future trade problems with the U.S. [5]. It remains to be seen if the Chinese will ever move away from their predatory practice. China is looking toward the future when environmental concerns will come into the picture, for example, China now invests more in green energy sources than does the U.S. [6].

Further dampening meaningful sanctions against Iran, Russia announced it would help complete an Iranian civil nuclear power station [7]. As expected, the President concluded a nuclear arms reduction treaty with Russia; however, China is not part of the agreement [8]. Thus, while the U.S. must reduce its nuclear weapon inventory, China is free to continue its modernization and expansion.

1. Twaronite, Lisa, Market Watch, *Between a yuan and a hard place*, March 17, 2010.
2. Dyer, Geoff, Financial Times, *World Bank raises China growth forecast*, March 17, 2010.
3. Wheatley, Alan, Reuters, *U.S. tells China yuan issue is of "real concern"*, March 18, 2010.
4. Palmer, Doug, Reuters, *China trade blamed for 2.4 mln lost US jobs-report*, March 23, 2010.
5. Rabinovitch, Simon, and Chang, Langi, Reutersm *China makes its case for a steady yuan*, March 28, 2010.
6. Hargreaves, Steve, CNN Money, *China trouncing U.S. in clean energy investing*, March 25, 2010.
7. Dombey, Daniel, and Gorst, Isabel, Financial Times, *Putin vexes US over Iran nuclear power*, March 18, 2010.
8. Baker, Peter, and Cooper, Helene, New York Times, *Obama Seal Arms Control Deal With Russia*, March 26, 2010.

It is our business to manufacture for ourselves whatever we can, to keep our markets open for what we can spare or want; and the less we have to do with the amities or enmities of Europe, the better–Thomas Jefferson

Counterfeit Devices

The Department of Commerce released a report of counterfeit electronic devices [1]. The report follows a 2007 incident with the U.S. Department of the Navy, Naval Air Systems Command (NAVAIR) in which thousands of counterfeit chips entered the supply system.

Highlights from the report include: lack of traceability in the supply chain is commonplace; insufficient chain of accountability within organizations; most DOD organizations do not have policies in place to prevent counterfeit parts from infiltrating their supply chain; and all elements of the supply chain have been directly impacted by counterfeit electronics. The data collected shows the number of suspected/confirmed counterfeit part incidents rising dramatically over four years to a level approaching 10,000 annually. Counterfeit microelectronics incidents increased from 3,040 in 2005 to 7,114 in 2008. What's more, counterfeit versions of components on the Qualified Products List (QPL) categories present a particular concern for the U.S. defense supply chain. Not surprisingly, most of the counterfeit devices came from China. Three distributors specifically mentioned encountering companies set up in the United States and Canada to sell parts from China in order to avoid association with parts from that region.

The most common method for discovering the counterfeit device was due to "returned due to defective." Of particular concern, few instances of counterfeit devices were reported to Federal authorities; indicating a larger problem exists. Moreover, microprocessors were the most common counterfeit microelectronic component.

1. U.S. Department Of Commerce, Bureau Of Industry And Security, Office Of Technology Evaluation, *Defense Industrial Base Assessment: Counterfeit Electronics*, January 2010.