Femtosecond®

www.femto-second.com

IN THE NEWS

VOLUME 1 ISSUE 12

JUNE 15, 2008

When Software Controls Fail

The District of Columbia (D.C.) was recently rocked by the largest corruption case in the city's history. With losses estimated at $50 million, the D.C. government is planning to scrap the $135 million application rather than upgrade it [1]. Another report, suggests the system has a reliability issues that often requires user to duplicate reports by hand [2]. This comes at a time when auditors have identified up to $2 million in potential overcharges by the software application company [3]. The company performing the work for the district government has been in the news before. Congresswoman Rosa L. DeLauro (D-CT) , criticized the company for having its corporate headquarters in Bermuda thereby reducing its US federal tax burden [4].

A brief history of the case follows: The scam went on for seven years until a bank employee last summer noticed irregularities in the checks [5]. Two tax employees and six others were charged with conspiring to steal more than $20 million in bogus property tax refunds [6]. Last December, D.C. Chief Financial Officer Natwar Gandhi apologized for the scandal and promised to correct the problems [7]. Jacqueline C. Wright, an employee of the tax office and Michael Clark were charged with stealing $180,000 in a tax refund scam [8].

Given the scope of the DC tax application crisis, why was the fraud only uncovered following a Sun Bank teller in Bowie (Maryland) questioned a refund check [9]? Large applications should include dual controls and have powerful audit capabilities. So what went wrong?

1. Keating, Dan, The Washington Post, *Tax Suspect's Guidance on Software Left D.C. at Risk*, June 10, 2008.
2. WTOP/Associated Press, *D.C. scraps $120 million tax system*, May 6, 2008.
3. Keating, Dan, The Washington Post, *Payments To Firm Deemed Improper*, May 22, 2008.
4. Statement of the Hon. Rosa DeLauro on $10 Billion Accenture Government Contract, http://www.house.gov/delauro/press/2004/accenture_06_01_04.html.
5. Barakat, Matthew, Associated Press, *Tax Scandal Court Files Look*

(Continued on page 2)

Global Bank Regulation

The US has a staggering trade deficit compounded by the high energy costs. There is a concern that the rest of the world may not continue to fund the US account deficit at the current exchange rates [1]. If this were to happen either interest rates would increase or the imports could not be purchased.

The large banks have had to make confessions and now regulators must decide how to implement reforms [2]. Overseas the Bank of England rate-setter, Paul Tucker, is suggesting better international financial regulation should avoid excesses highlighted in the current crisis [3]. One concern is that if large financial institutions believe the Government will bail them out, they are more likely to make riskier loans [4].

1. Politi, James, and Tett,

(Continued on page 2)

Inside this issue:

Special points of interest:

- 2.2 million hospital billing records stolen in Utah
- One woman bilks Government out of $105 million in Medicare fraud
- Utilities vulnerable

When Software Controls Fail

(Continued from page 1)

Like Posh Christmas List, December 14, 2007.

6. WTOP/Associated Press, *Congress Nixes Raise for Gandhi*, June 19, 2008.
7. WTOP/Associated Press, *CFO Gandhi Apologizes for Tax Office Scandal*, December 20, 2007.
8. WTOP/Associated Press, *Another D.C. tax scandal: Cash used for home improvements*, June 4, 2008.
9. WJLA, *D.C. Tax Fraud Scandal Keeps Growing*, November 14, 2007

Secure Information Exchange

Securely exchanging information amongst assorted parties has always been a security goal. In an effort to identify better solutions, the department of Defense is funding five year information sharing research at six universities [1]. In congress, there are several bills designed to make DHS shared information more readily available [2].

To control sensitive information it first helps to know what is and is not sensitive. For years, military (and other) organizations used *Sensitive but Unclassified (SBU)* as a designator. The President signed a memorandum to replace SBU with *Controlled Unclassified Information (CUI)* [3]. However, the new information designation currently is lacking specifics [4]. The President is adding the CUI designation to information that is part of the administration's *Information Sharing Environment (ISE)*, that was defined in response to the Intelligence Reform and Terrorism Prevention Act of 2004 [5].

Information exchange is not limited to online transaction. Reader may recall stories about lost backup tapes containing sensitive information. The latest case in point is at the University of Utah where 2.2 million billing records were stolen from a courier's vehicle [6]. In an effort to retrieve the tapes, a $1,000 reward is being offered, no questions asked [7]. What are the odds the take was encrypted?

Overseas, seven pages of "UK Top Secret" terrorism documents were left on a train [8]. This is followed by a second batch of papers was also discovered on a train [9].

> *Insanity: doing the same thing over and over again and expecting different results.—Albert Einstein*

1. Jackson, William, GCN, *DOD funds research into info sharing*, June 10, 2008.
2. Federal Computer Week, *Bills would give more access to DHS data*, June 11, 2008.
3. Bush, George W., Memorandum For The Heads Of Executive Departments And Agencies, *Designation and Sharing of Controlled Unclassified Information (CUI)*. May 9, 2008.
4. UPI, *New data classification lacks specifics*, May 19, 2008.
5. Bush, George W., *Message to the Congress of the United States on Information Sharing*, December 16, 2005.
6. Associated Press, *Utah hospital billing records stolen from courier*, June 10, 2008.
7. The Salt Lake Tribune, *U of U medical records stolen, 2.2 million patients' data at risk*, June 11, 2008.
8. Dodds, Paisley, Associated Press, *Secret al-Qaida, Iraq files found on British train*, June 13, 2008.
9. CNN (London), *Report: More secret documents found on London train*, June 14, 2008.

Global Bank Regulation

(Continued from page 1)

Gillian, Financial Times, *NY Fed chief urges global bank framework*, June 8, 2008.

2. Reuters, *Tougher tasks ahead in bid to fix world's financial markets*, June 13, 2008.
3. Thompson Financial (London), *BoE's Tucker says more financial regulation needed to avoid future credit crises*, June 13, 2008.
4. Tessler, Joelle, Associated Press, *Paulson Sits On Fiscal Hot Seat*, June 14, 2008.

Bad Actors

In Florida, a woman used her laptop to file 140,000 Medicare claims thereby bilking the Government out of $140 million [1]. Exactly what king of audit controls allow 140,000 unchecked claims?

A California hacker pleaded guilty to launching a bot-net attack that nearly shut down an anti-phishing web site [2]. A hacker in Florida was sentenced to 41 months for running a bot-net that installed unauthorized advertising software [3].

Overseas, in a clear challenge to law enforcement, a hacker took down a police web page [4].

1. Johnson, Carrie, Washington Post, *'Rags to riches' through Medicare fraud*, June 13, 2008.
2. McMillian, Robert, IDG News Service, *Hacker Pleads Guilty to Attacking Anti-phishing Group*, June 10, 2008.
3. Kirk, Jeremy, IDG News Service, *U.S. hacker gets 41 months for running rogue botnet*, June 12, 2008.
4. BBC News, *Hacker brings down police website*, June 10, 2008.

This Week's Financial News

The trade deficit for April grew to $60.9 billion, including $29.3 in imported oil [1]. The deficit also included $20.2 billion with China, down from the same period last year but up from March [2]. Lehman Brothers Holding Inc., the 4th largest investment bank, reports unexpectedly large second quarter loss of $2.8 billion [3].

Weeks after the FDIC closed the ANB Financial National Association in Bentonville, brokered certificate of deposit were still not available to depositors [4]. Hopefully, depositors will not lose confidence in the FDIC.

In other news, three were sentenced in North Carolina on a $1.2 million bank fraud scheme [5]. In Ohio, a developer bilked several banks and companies out hundreds of thousands of dollars [6]. In Connecticut, A former vice president of Bank of America and Fleet Bank pleaded guilty to bribery and fraud that resulted in a $1.5 million loss [7].

1. Crutsinger, Martin, Associated Press, *Trade deficit jumps to highest level in 13 months*, June 10, 2008.
2. Kuritenbach, Elaine, Associated Press, *China May trade surplus down 10 percent on imports*, June 11, 2008.
3. Bruno, Joe, Associated Press, *Lehman raising $6B in capital, expects $2.8B loss*, June 9, 2008.
4. Tompor, Susan, Detroit Free Press, *Consumers with brokered CDs find money at risk if bank fails*, June 9, 2008.
5. The News Observer (Raleigh), *Three sentenced in bank fraud scheme*, June 11, 2008.
6. Pramik, Mike, The Columbus Dispatch, *Developer jailed on bank-fraud charges,* June 11, 2008.
7. Gershon, Eric, Hartford Courant, *Former Bank Executive Pleads Guilty To Bribery, Fraud*, June 13, 2008.

We can never tell what is in store for us. – Harry S. Truman

More Olympics Warning

Travelers to the Olympics are cautioned that if you are of interest to the Chinese government, you are likely to have you laptop compromised, even during a security screening [1]. This warning comes as congressmen Frank Wolf (Virginia) and Chris Smith (New Jersey) allege computers in their offices were hacked by sources in China [2]. On the other side, China has denied any involvement in hacking the Congressional computers [3].

For the 2008 Olympics, china has issued rules for travelers. The 57 rules include, baring anyone with mental illness, restricting travel to certain places (including Tibet), and no displaying "offensive" slogans [4].

1. Eisler, Peter, USA Today, *Olympic visitors' data is at risk*, June 11, 2008.
2. Yost, Pete, and Jakes Jordan, Laura, Associated Press, *2 lawmakers say computers hacked by Chinese*, June 11, 2008.
3. Associated Press (Beijing), *China denies hacking into US computers*, June 12, 2008.
4. CNN (Beijing), *China lists Olympic rules for foreigners*, June 3, 2008.

Supercomputers

As technology becomes more powerful and more available, the security approaches used to protect IT assets must evolve. Consider the security experts that once claimed the Data Encryption Standard would be strong enough for protecting information for the foreseeable future. The simple controls of yesterday are no match for the processing power than can be applied against legitimate infrastructures.

Case in point, a supercomputer called *Roadrunner* has reached a computing milestone by processing 1.026 quadrillion calculations per second [1]. So if a computer can perform 1.0 quadrillion calculations per second, this means it takes 1 Femtosecond to calculate an instruction.

The Roadrunner still has a large footprint. For example, it weighs a half a million pounds, uses 296 racks totaling 10,000 square feet, and consumes 2.8 megawatts of power [2]. We should expect to see supercomputers to evolve for the foreseeable future.

1. Markoff, John, International Herald Tribune, *Supercomputer sets record*, June 9, 2008.
2. Miller, Erica, KAAL, *IBM's Roadrunner New Supercomputer*, June 12, 2008.

Critical Infrastructure

In Newsletter issue 10, we discussed a report that hackers China may have contributed to two US power blackouts. A new report indicates there is a vulnerability that hackers could exploit in the software that controls water treatment plants, natural gas pipeline, and other utilities [1].

Perhaps the most visible utility is the nuclear power generating plants. While the full protection mechanisms are not widely publicized, we can get some insight into potential problem areas. For example, a nuclear plant in Georgia was shut down for 48 hours following a "cyber incident" [2]. Apparently, software was updated on a single computer that culminated in the shutdown [3]. A Southern California Edison 1,070 megawatt nuclear reactor was shut down on June 5 while returning from a brief maintenance outage [4]. In New York, the emergency shutdown of a reactor at the Indian Point nuclear power plant was caused by a digital camera [5].

> *A good plan executed today is better than a perfect plan executed at some indefinite point in the future.–General George Patton Jr*

1. Robertson, Jordan, Associated Press, *Security hole exposes utilities to Internet attack*, June 11, 2008.
2. UPI, *Cyber malfunction halts nuclear plant*, June 6, 2008.
3. Krebs, Brian, Washington Post, *Software Update Prompts Nuclear Plant Shutdown*, June 5, 2008.
4. Reuters, *SCE Calif. San Onofre 2 reactor shut*, June 6, 2008.
5. WNYC, *Digital Camera Blamed For Indian Point Shutdown*, June 12, 2008.

Identity Fraud

In Colorado, auditors discovered 48,000 dead people still had valid driver's licenses [1]. In Florida, a man was sentenced to 8 1/2 years for identity theft and wire fraud that affected a financial institution that funded $6 million in mortgages [2]. In Idaho, a Boise Cascade employee was charged in a wire fraud and identity theft scheme that defrauded the company of $185,000 [3]. In New Jersey, a former employee of the commerce Bank was indicted in a scheme where five identities were and $100,000 worth of goods were stolen [4].

1. Morson, Bernu, Rocky Mountain News, *Driver's license agency criticized on prevention of fraud*, ID theft, June 10, 2008.
2. Tampa Bay Business Journal, *U.S. Attorney: fraud used identity theft to fund $6M in mortgages*, June 12, 2008.
3. Idaho Statesman, *Former Boise Cascade employee charged in wire fraud, identity theft case*, June 13, 2008.
4. Graham, Kristen A., Philadelphia Inquirer, *Identity-theft charges face a N.J. woman*, June 14, 2008.