Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 5

April 27, 2008

The International Banking Industry

Banks continue to report losses attributed to the mortgage crisis. Some domestic examples include: The Bank of America reported a 77% drop in quarterly earnings [1]; The Mercantile Bank reported a quarterly loss of $201 million versus a $20.5 income from the same quarter last year [2]; and The National City Corp reported a $171 million quarterly loss [3].

While US banks continue to report losses, the impact to the banking industry is not confined to the United States. Credit Suisse, the second largest Swiss bank, reported a quarterly write down of $5.3 Billion resulting in a $2.1 billion loss [4]. The India State run bank of Commerce reported a quarterly loss [5]. Italy's largest bank UniCredit, reported losses doubled to $1.07 billion for the quarter [6]. The Royal Bank of Scotland reported an additional $11.7 billion in mortgage related losses [7]. The nine month loss for the Swiss bank, UBS, is estimated at $37.4 billion [8]. To address continuing problems, foreign governments are expanding efforts to minimize chaos in the financial markets. For example, the Bank of England is allowing up to $100 billion for exchanging mortgage based securities [9]. In tandem foreign banks are coming under increased pressure to do more for bank customers [10]. Correspondingly, following the loss of laptop computers that contained unencrypted sensitive information on 10,000 customers, the Bank of Ireland has set up a customer hotline [11].

Closer to home, the Heritage bank in Georgia, reported a $923,000 charge for deposit account fraud culminating in a total quarterly loss of $505,000 [12]. The Heritage report is attention-grabbing since loss attributed to deposit account fraud is rarely reported. In an apparent paradox, the Securities and Exchange Commission (SEC) turned down a congressional inquiry as to why an investigation into the Bear sterns collapse was halted [13]. The SEC normally does not report on ongoing investigation (or the lack thereof) so the congressional inquiry may not be solid. It seems likely that the SEC would investigate the collapse of Bears Sterns unless another investigating Government agency has jurisdiction. In a separate case, the Justice Department and SEC are investigating Ralph R. Cioffi, the former manager of the two Bear Stearns hedge funds to determine if he misled investors [14]. Regulators at the Office of the Comptroller of the Currency (OCC) are examining information received from other country bank exploits. For instance, following the fraud loss of the SocGen bank in France by a 31 year old insider, US banks are examining internal controls [15]. The SocGen fraud now estimated at $7.8 billion is estimated to be the largest known fraud ever to hit a financial institution [16].

In other news, a Florida man was convicted of defrauding the import-export bank of almost $30 million in fraudulent loan transactions [17]. Wachovia will pay as much as

(Continued on page 2)

HSPD-12 and Match on Card

The Office of Management and Budget (OMB) is requiring agencies improve their Homeland security Presidential Directive 12 (HSPD-12) reporting [1]. While agencies continue to lag in reporting, there are new features being tested.

The NIST conducted tests of biometric match on card with verification completed within a few seconds [2]. The implementation includes encryption between the card and the reader. As biometric implementations progress, others are claiming that the benefit of fingerprints is they cannot be copied [3]. However, consider the discussion in newsletter (vol. 1 issue 2) where the Chaos Computer Club is maintaining a fingerprint database of high visibility Government people. Unlike a PIN, your

(Continued on page 2)

Inside this issue:

Special points of interest:

- Head of 2010 Census to retire
- Sub-prime crisis aided first person crime

HSPD-12 and Match on Card

(Continued from page 1)

biometric never changes. Is copying a fingerprint and spoofing a reader really impossible? If we look at currency and product counterfeiting the criminal sophistication used cannot be discounted. If we assume that cybercriminals will not find a way to copy fingerprints we are likely in for unpleasant surprises.

1. Hardy, Michael, FCW, *OMB: Agencies HSPD-12 postings improve*, April 23, 2008.
2. csrc.nist.gov/publications/nistir/ir7452/NISTIR-7452.pdf
3. Government Technology, *NIST Shows On-card Fingerprint Match Is Secure*, Speedy, April 3, 2008.

The International Banking Industry

(Continued from page 1)

Most Americans have no real understanding of the operation of the international money lenders. The accounts of the Federal Reserve System have never been audited. It operates outside of the control of Congress and manipulates the credit of the United States.–Barry Goldwater

$144 million to settle an investigation that accused the bank of allowing telemarketers to steal millions of dollars [18]. The Chicago-based MB Financials Inc. discovered a customer falsified various reports sent to the bank necessitating the bank to set aside $22.5 million for potential loss [19].

The sub-prime crisis has facilitated first party crime where synthetic identification and qualification without human intervention are the norm [20]. With the lack of identity authentication, bogus paper, and other issues of integrity, perhaps the damage is sufficient to consider controls based on strong identification and authentication. Clearly some of the damage attributed to the sub-prime crisis can be attributed to cybercrime. What remains to be determined is how much.

1. Augstums, Ieva M., AP, *Bank of America's 1Q profit shrinks amid economic worries*, April 21, 2008.
2. Tampa Bay Business Journal, *Mercantile Bank parent posts $201 million 1Q loss*, April 23, 2008.
3. Bansal, Paritosh, Reuters, *National City raising $7 billion; shares sink on loss*, April 21, 2008.
4. Sigrist, Daniela, AP, *Credit Suisse Q1 write-downs of $5.3B drives $2.1B loss*, April 24, 2008.
5. Reuters, New Delhi, *Oriental Bank posts Q4 loss on extraordinary items*, April 23, 2008.
6. Migliaccio, Alessandra, Bloomberg, *UniCredit Says Trading Loss Doubled in First Quarter* , April 23, 2008.
7. Associated Press, *Shares of commercial banks mostly fall after RBS posts additional $11.7 billion loss*, April 22, 2008.
8. AP, *UBS blames subprime loss on excessive risk-taking*, April 21, 2008.
9. Jolly, David, and Dougherty, Carter, The New York Times, *Bank of England Outlines Its Bailout Plan*, April 21, 2008.
10. BBC News, *Call for bank action on ID theft*, April 24, 2008.
11. BBC News, *Helpline set up over bank breach*, April 22, 2008.
12. Rauch, Joe, Atlanta Business Chronicle, *Heritage Bank flips to loss on fraud, residential losses*, April 21, 2008.
13. Reuters, *SEC refuses to say why Bear enquiry dropped: report*, April 23, 2008.
14. Goldstein, Matthew, Business Week, *The Feds' Subprime Suspect*, April 23, 2008.
15. Poirier, John, and Graybow, Martha, Reuters, *U.S. Banks examine controls after SocGen*, February 6, 2008.
16. Matlack, Carol, Business Week, *SocGen's Changing of the Guard*, April 21, 2008.
17. UPI, *Florida man sentenced for bank fraud*, April 23, 2008.
18. Duhigg, Charles, The New York Times, *Wachovia settles in fraud case*, April 26, 2008.
19. Yerak, Becky, Chicago Tribune Web Edition, *MB Financial uncovers fraud, sets aside more for losses*, April 26, 2008.
20. SC Magazine, *First party fraud*, April 1, 2008.

Phishing

Hardly a week passes without news of yet another phishing attack. The latest is a bogus IRS letter for your tax rebate [1]. Overseas, the number of phishing attacks in the United Kingdom doubled during the first quarter however the reported loss decreased by one third [2]. This decrease is probably due to heightened awareness on the part of users.

The phishing cybercriminals are expanding their attacks. One group that surfaced in 2004, the Rock Phish gang, has devised a way for the Zeus Trojan to be installed in vulnerable machines without submitting information [3]. This attack works by duping the victim to go to the phishing site; infecting the computer even if no other action is taken; and taking screen scrapes and capturing passwords [4].

1. Jackson, William, Government Computer News, *Phishing scam uses IRS rebate line to reel in victims*, April 23, 2008.
2. Broersma, Matthew, Techworld, *Phishing Attacks Double in U.K.*, April 20, 2008.
3. Kirk, Jeremy, InfoWorld, *Rock Phish gang adds second punch to phishing attacks*, April 21, 2008.
4. Dignan, Larry, ZDnet, *RSA finds new malware enhanced phishing technique*, April 21, 2008.

China

China continues to march toward a global dominance in business and technology. There are now 221 million Internet users in China outnumbering the US [1]. China is also advancing in the area of space exploration and has built lunar rover prototypes [2]. With China's elevated presence in science and technology comes the risks that other countries have struggled with. For example, China is worried that hackers will launch attacks during the Olympics [3]. This is consistent with the Interpol warning that Al–Qaeda may be planning a terrorist attack [4].

With the technology advancements comes the technical challenges in maintaining Web censorship. Currently, there is an effort to control web content but there are active attempts by the masses to circumvent the censorship controls [5].

1. AFP, *China's online population exceeds the US: report*, April 24, 2008.
2. Kyodo, Beijing, *China builds lunar rover prototype: report*, April 23, 2008.
3. Lemon, Sumner, IDG News Service, *China Worries Hackers Will Strike During Beijing Olympics*, April 23, 2008.
4. AFP, *Interpol chief warns of Olympic terror threat*, April 25, 2008.
5. Wiseman, Paul, USA Today, *Cracking the 'Great Firewall' of China's Web censorship*, April 24, 2008.

I am not an Athenian or a Greek, but a citizen of the world. – Socrates

Scaled Back Census Test

In the latest twist with the Census, a previously scheduled test will be scaled back [1]. The Bureau of Census will revert to pencil and paper, at a significantly increased cost [2]. Perhaps because of these problems, Preston Jay Waite, in charge of the 2010 census, is retiring [3]. The sad part is that there is still time to correct the original problems but clearly, the Department of Commerce has little confidence in the success of modernization. So what will the quality of the next census be like?

1. Burke, Garance, Associated Press, *Test run for 2010 census is scaled back, worrying experts*, April 24, 2008.
2. Ohlemacher, Stephen, AP, *Tech Problems Blamed on Census Bureau*, April 9, 2008.
3. UPI, *Top Census official retiring*, April 24, 2008.

Cybercrime

Attorney General Michael Murskey listed a number of areas that organized criminal enterprises are targeting. The list included cyberspace to jeopardize the stability of financial investment markets and the manipulation of security exchanges [1]. There are currently 120 prosecutors and FBI agents and analysts are working on organized crime issues [2]. In contrast, FBI Director Mueller has almost 270 agents working nationwide on the $20 billion per year child pornography black market [3]. Based on these numbers, the cybercrime effort looks understaffed.

The FBI is seeking new laws to assist in their investigatory work. Director Mueller, has requested congress provide the legal tools to allow monitoring of illegal activity on networks outside Government [4].

1. Frieden, Terry, CNN, *Criminals target energy, financial markets*, Mukasey says
2. Johnson, Carrie, Washington Post, *Justice Dept. Sees Surge In Global Crime Networks*, April 24, 2008.
3. Ryan, Jason, ABC News, *120 prosecutors and FBI agents and analysts are working on organized crime issues*, April 23, 2008.
4. Broache, Anne, cnet news, *FBI wants widespread monitoring of 'illegal' Internet activity*, April 23, 2008.

The cost of IT Security

There is no security on this earth, there is only opportunity.–General Douglas MacArthur

There are costs associated with security controls and losses. Zero-day attacks render many security controls ineffective until a fix is made available. Still, the estimated cost for security software alone is $10.5 billion [1]. To appreciate what the threat is, there are currently over one million malicious code threats [2].

The number of threats is increasing and there is no end in sight. Many have resisted stronger security controls due to the complexity and cost. The question here is can we afford not to beef up security? As long as cybercrime is profitable, the threat will remain a dominant concern.

1. Yu, Eileen, Business Week, *Security Software to Hit $10.5 Billion*, April 25, 2008.
2. BBC News, *Computer viruses hit one million*, April 10, 2008.

Critical Infrastructure Protection

Homeland security Presidential Directive 7 (HSPD-7) gives the Department of Homeland Security (DHS) the lead role in protecting vital infrastructure [1]. It should be obvious that protecting the physical infrastructure requires cyber protection.

Some have suggested a perimeter defense with expanded DHS and DoD roles [2]. The idea of a countrywide security perimeter is not new. Perhaps the most ambitious perimeter defense is the Chinese censorship firewall [3]. Overseas, some have pointed out that Information Security professionals are rarely involved in the early development of critical infrastructure components [4].

With countries such as China, Russia, and India expanding their presence on the Internet, trying to protect against systemic security vulnerabilities seems a lost cause. Perhaps a better solution is to better integrate security into the IT resources protecting the physical infrastructure.

1. hwww.whitehouse.gov/news/releases/2003/12/20031217-5.html
2. Bain, Ben, Federal Computer week, *Critical infrastructure central to cyber threat*, April 24, 2008.
3. Scheer, Peter, International Herald Tribune, *Inside the Great Firewall*, April 18, 2008.
4. Jaques, Robert, Infosec Europe, *Critical infrastructure open to IT security threats*, April 21, 2008.