Trends in Financial (cyber) Crimes

Raj Goel, CISSP
Chief Technology Officer
Brainlink International, Inc.
raj@brainlink.com / 917-685-7731

Raj Goel, CISSP



Raj Goel, CISSP, is an Oracle and Solaris expert and he has over 22 years of experience in software development, systems, networks, communications and security for the financial, banking, insurance, health care and pharmaceutical industries. Raj is a regular speaker on HIPAA, Sarbanes-Oxley,PCI-DSS Credit Card Security, Information Security and other technology and business issues, addressing diverse audiences including technologists, policy-makers, front-line workers and corporate executives.

He also works with community and professional organizations such as the InfraGard, ISC2, and TibetAid.org, Association of Cancer Online Research - ACOR.org.

A nationally known expert, Raj has appeared in over 20 magazine and newspaper articles worldwide, including ***Entrepreneur Magazine***, ***Business2.0*** *and* ***InformationWeek***, and on television including ***CNNfn*** and ***Geraldo At Large.***

Agenda

- Spyware / SPAM / Phishing
- Fraud makes the world go around
  - Real Estate frauds
  - Fake Receipts
  - Fake Equipment
- Credit Card Theft
- Future Crime – Click Fraud

2005 – 2009 summary

hacker	***256,044,318***	*
stolen computer	***100,865,672***	
insider	***31,039,442***	
tape lost	***20,735,379***	
unsanitary web practice	***11,987,329***	
poor process	***6,378,201***	
unshredded paper	***2,270,247***	
hd stolen	***723,200***	
social engineering	***714,000***	**
crimeware	***197,000***	***
unsanitized drives	***113,183***	
briefcase stolen	***41,460***	
Total	**431,109,431**	

* Is it really hacking, or dishonest insiders or poor processes?

** Data collection firms allowed criminals to setup customer accounts and sold them data

*** A custom virus against a university,
and unknown how many PCs were
infected via
Google Ads serving malware

Lose Data, Lose Customers The Ponemon Institute surveyed 14 different companies. The average data loss was 100,000 records. The most costly aspect by far was the loss of existing customers. Here is the breakdown:

ACTIVITY	DIRECT COSTS	INDIRECT COSTS	LOST CUSTOMER COSTS	TOTAL COSTS
Detection & Escalation				
– Internal investigation	$19,000	$488,000	N/A	$507,000
– Legal consulting	463,000	51,000	N/A	514,000
Notification				
– Letters	547,000	193,000	N/A	740,000
– E-mails	5,000	N/A	N/A	5,000
– Telephone	913,000	105,000	N/A	1,018,000
– Published media	48,000	N/A	N/A	48,000
– Web site	3,000	N/A	N/A	3,000
Ex-Post Response				
– Mail	4,000	3,000	N/A	7,000
– E-mails	1,000	1,000	N/A	2,000
– Internal call center	287,000	479,000	N/A	766,000
– Outsourced call center	27,000	N/A	N/A	27,000
– Public or investor relations	289,000	14,000	N/A	303,000
– Legal defense services	1,288,000	N/A	N/A	1,288,000
– Free or discounted services	810,000	N/A	N/A	810,000
– Criminal investigations	286,000	13,000	N/A	299,000
Lost Business				
– Lost existing customers	N/A	N/A	6,728,000	6,728,000
– Lost new customers	N/A	N/A	730,000	730,000
AVERAGE COST PER COMPANY	**$4,990,000**	**$1,347,000**	**$7,458,000**	**$13,795,000**
PER LOST RECORD COST	$50	$14	$75	$138

SOURCE: PGP CORP.

The Cost of Carelessness 12/5/2005 - http://www.cioinsight.com/article2/0,1540,1906158,00.asp

Cost of Breaches 2005-2009

Year	Direct Cost	Indirect Cost	Lost Customer Cost	Total Costs
2005	50	14	**74**	**138**
2006	50	14	**118**	**182**
2007	50	14	**133**	**197**
2008	50	14	**138**	**202**
2009	50	14	**140**	**204**

Other findings:

Not 1st time for majority of companies – 84% repeat offenders

1st timers cost: $ 243/record, Experienced Victims: $ 192/record

Churn Rates: Average 3.6% / Healthcare 6.5% / Financial Services 5.5%

Healthcare cost: $ 282/record / Retail: $ 131/record

88% breaches due to insider negligence, 44% due to external parties

Source: http://www.networkworld.com/news/2009/020209-data-breach.html

Attack of the Zombie computers

Security researchers have been concerned about botnets for some time because they automate and amplify the effects of viruses and other malicious programs.

What is new is the vastly escalating scale of the problem — and the precision with which some of the programs can scan computers for specific information, like corporate and personal data, to drain money from online bank accounts and stock brokerages.

“It’s the perfect crime, both low-risk and high-profit,” said Gadi Evron, a computer security researcher for an Israeli-based firm, Beyond Security, who coordinates an international volunteer effort to fight botnets. “The war to make the Internet safe was lost long ago, and we need to figure out what to do now.”

Last spring, a program was discovered at a foreign coast guard agency that systematically searched for documents that had shipping schedules, then forwarded them to an e-mail address in China, according to David Rand, chief technology officer of Trend Micro, a Tokyo-based computer security firm.
[...] consensus among scientists is that botnet programs are present on about 11 percent of the more than 650 million computers attached to the Internet.
- NY Times, January 7, 2007

Economics of SPAM

The Securities and Exchange Commission said that its actions to freeze proceeds from a suspected high-tech pump-and-dump stock scheme and its suspension of stock trading on 35 companies touted in spam...

Dimitri Alperovitch, principal research scientist at Secure Computing, described such spamming and pump-and-dump schemes as part of the same unified spam economy.

Profits from that economy start at botnets or zombie PCs, which are rented out to spammers. Spam goes out touting the value of a chosen company. Excited victims buy into the scheme and buy up stocks in the touted companies. The spammer within a few days sells the stock, pocketing a tidy profit, leaving victims with stocks that are virtually worthless.

"A lot of these guys we believe are renting botnets from spammers distributing Viagra and other types of spam," Alperovitch said in an interview with eWEEK. "A lot [of the botnet controllers] may be getting paid in … the stock of the company they're trying to promote. They can use the increased price of the stocks to sell it off and make their profit that way."

With the ill-gotten profit, he said, the spammers/pump-and-dumpers then buy stock in another company whose value they will tout, and the cycle begins anew.

Secure Computing estimates that 30 percent of all spam is stock spam, and spam itself makes up "well over 90 percent of all e-mail," Aperovitch said. [...]that is up from over 70 percent a year ago.
- eWeek, March 11, 2007

Priceline, Travelocity, and Cingular fined for using adware

Priceline, Travelocity, and Cingular, three high-profile companies that advertised through nuisance adware programs have agreed to pay fines and reform their practices, according to the New York Attorney General.

“Advertisers will now be held responsible when their ads end up on consumers’ computers without full notice and consent,” Andrew Cuomo said. “Advertisers can no longer insulate themselves from liability by turning a blind eye to how their advertisements are delivered, or by placing ads through intermediaries, such as media buyers. New Yorkers have suffered enough with unwanted adware programs and this agreement goes a long way toward clamping down on this odious practice.”

- PressEsc.com January 29, 2007

ChronoPay – Russian Government + Criminals

"If your Windows PC has been hijacked by fake anti-virus software or "scareware" anytime in the past few years, chances are good that the attack was made possible by **ChronoPay**, Russia's largest processor of online payments.

ChronoPay employees created two companies in Cyprus that would later be used in processing rogue anti-virus payments: **Yioliant Holdings**; and the strangely named **Flytech Classic Distribution Ltd.** ChronoPay emails show that employees also paid for domains **software-retail.com** and **creativity-soft.com**, rogue anti-virus peddling domains that were registered in the names and addresses of Yioliant Holdings and Flytech, respectively. Finally, emails also show that ChronoPay paid for the virtual hosting and telephone support for these operations."

- http://krebsonsecurity.com/tag/chronopay/
- http://krebsonsecurity.com/wp-content/uploads/2011/03/csoft.txt

Spyware - Israel's TrojanGate

- “Executives of top telecom firms accused of spying on each other. A jealous ex-husband suspected of monitoring his former in-laws. Private investigators implicated in computer-hacking-for-hire; one now involved in a possible attempted suicide. So much bad publicity, **government officials worry it might impact the entire nation’s economy.**

- Published reports indicate mountains of documents have been stolen from dozens of top Israeli firms. **Some 100 servers loaded with stolen data have been seized.**”

- - MSNBC, June 9, 2005 http://www.msnbc.msn.com/id/8145520/

Spyware - Japan's Winny P2P

- “in particular, a military agency was forced to admit that classified information from the Maritime Self Defence Force was uploaded by a computer with winny software installed on it.
- Following this, ANA (All Nippon Airlines) were also the victims of an embarrassing data leak, with passwords for security-access areas in 29 airports across Japan being leaked over the program. This follows a similar incident from JAL Airlines on 17th December 2005, after a virus originating from Winny affected the computer of a co-pilot.
- Arguably the biggest winny-related leak however, is that of the Okayama Prefectural Police Force, whose computer leaked data on around 1,500 investigations. This information included sensitive data; such as the names of sex crime victims, and is the largest amount of information held by Japanese police to have ever leaked online.”
- - WikiPedia - http://en.wikipedia.org/wiki/Winny

Spyware - Bank Of America / Joe Lopez lawsuit

- " A Miami businessman is suing Bank of America to recover **$90,000 that he claims was stolen and diverted to a bank in Latvia after his computer was infected by a "Trojan horse"** computer virus.
- Although consumers are routinely hit with "phishing" E-mails carrying bank logos intended to dupe them into revealing IDs and passwords, this

BOA settled with Joe Lopez, after negative publicity, in an undisclosed settlement.

- In a complaint filed earlier this month, Joe Lopez, owner of a computer and copier supply business, **accused Bank of America of negligence and breach of contract** in not alerting him to the existence of a virus called "coreflood" prior to April 6, 2004, the date the alleged theft took place." - http://www.informationweek.com/showArticle.jhtml?articleID=60300288

Spyware - Sony's DRM Rootkit

- US government officials took Sony BMG to task over its controversial use of rootkit-style copy protection at a security conference this week. **If the technology proves harmful to consumers, tougher laws and regulations might be proposed**, a senior Department of Homeland Security exec warned.
- "Legislation or regulation may not be appropriate in all cases, but it may be warranted in some circumstances," said Jonathan Frenkel, director of law enforcement policy with the DHS's Border and Transportation Security Directorate.
- [...] DHS officials had a meeting with **Sony** BMG shortly after the story broke during which the entertainment **reps were read the riot act.** "**The message was certainly delivered in forceful terms that this was certainly not a useful thing,"** Frenkel said.
- Government officials are concerned that the rootkit tactic, if repeated, could leave consumers' systems open to hacker attack.
- - Feb 17, 2006 - http://www.theregister.co.uk/2006/02/17/rootkit/

Spyware - Sony's DRM Rootkit

- Oct 31, 2005 - Mark Russinovich, a security researcher, discovers that Sony's CDs install a rootkit
- Nov 3 – Sony releases rootkit remover. Ed Felten dismisses the rootkit remove as junk
- **Sony's rootkit used to defeat World of Warcraft's security**
- Nov 15 – Sony's rootkit uninstaller "create huge security hole"
- Nov 15 – Dan Kaminsky estimates Sony's rootkit has **infected 568,200 sites, including government and military networks.**
- Nov 16 – US-CERT, Dept of Homeland Security, advises: "**Do not install software from sources that you do not expect to contain software, such as an audio CD."**
- Nov 17 – Amazon offers refunds on infected Sony CDs. Nov 21, Army/Airforce exchange as well.
- **New York, Texas and Florida Attorney Generals sue Sony.**
- - boingboing.net
- Nov 10 – **2 Trojans target Sony's rootkit** - http://news.zdnet.co.uk/internet/security/0,39020375,39236720,00.htm
- Attorney fees & expenses exceed $ 4,000,000. Total costs to Sony unknown. - sonysuit.com

Spyware - Sony's DRM Rootkit
Anastacia CD costs retailer 1,500 Euros

- **Sep 14, 2009 – German Judge orders retailer to pay Plaintiff 1,500 Euros.**
- 200 Euros – 20 hours wasted dealing with virus alerts
- 100 Euros – 10 hours for restoring data
- 800 Euros – fees paid by Plaintiff to Computer Expert to repair his network
- 185 Euros – legal costs incurred by plaintiff

"The judge's assessment was that the CD sold to the plaintiff was faulty, since he should be able to expect that the CD could play on his system without interfering with it.

The court ordered the retailer of the CD to pay damages of 1,200 euros."

http://torrentfreak.com/retailer-must-compensate-sony-anti-piracy-rootkit-victim-090914/

http://www.heise.de/newsticker/Verkaeufer-muss-Schadensersatz-fuer-Sony-Rootkit-CD-zahlen--/meldung/145233

ID Theft – Bank Of America & Margaret Harrison

Margaret Harrison, a young wife and mother living in San Diego, first noticed the problem four years ago when she applied for unemployment.
[...] She investigated and found out a laborer named Pablo has been using her Social Security number. **And while Margaret pays for credit monitoring, she says the Equifax credit reporting bureau never noticed the problem until she told the agency.** Now Equifax has put a fraud alert on her account. And then there's this: Last month, the **Bank of America sent her a new debit card bearing her name and Pablo's picture!**
Margaret says the Bank of America claims it can't take any action against Pablo because he pays his bills on time — that her case is in what they call "a reactive state."

- MSNBC Feb 6, 2006 “Hey, that’s not me! A new wrinkle in ID theft”

Telemarketing Fraud

- Telemarketing fraud, predominately emanating from Canada, is a flourishing crime problem with estimated losses to U.S. elderly citizens exceeding $500 million per year.
- - http://www.fbi.gov/publications/financial/fcs_report052005/fcs_report052005.htm

- Telemarketing fraud - often consisting of credit card, loan and investment scams - continues to target both Canadian and US citizens. US losses due to this type of fraud are estimated at nearly $1 billion per year while Canadian losses are estimated at more than CDN $16 million. However, RCMP analysts estimate that only five percent of victims ever report to authorities, meaning that actual losses may approach CDN $295 million per year.
- - http://www.rcmp-grc.gc.ca/organizedcrime/octa_e.htm

Homeowners lose houses in property scams

Reviczky purchased the property at 220 Sheppard Ave. W. in 1980 for $67,500 to generate a rental income that would help pay for the education of relatives back in Hungary.
...
Reviczky could not believe his ears on June 26 when his neighbour, a real estate agent, told him she had noticed on the computer that he had sold his rental property in May.
...
Police believe Reviczky's most recent "tenants" forged his name on a power of attorney that purported to give a grandson named "Aaron Paul Reviczky" authority to sell the home on his behalf.
...
"I don't have a grandson named Aaron," Reviczky says. "I don't have any grandsons."
...
On May 15, "Aaron Paul Reviczky" sold the property on his behalf for $450,000 to a purchaser named Pegman Meleknia, who took out a mortgage of $337,500.
...
Reviczky's lawyer, Tonu Toome, says it was "very painful" to have to break the news to Reviczky that he may lose his house forever — even though he was an innocent victim of fraud — because Ontario law recognizes the transaction as valid where the purchaser is unaware of the scam.
- Toronto Star, August 26, 2006

ID Theft + Mortgage Fraud = House Stealing

The con artists start by picking out a house to steal—say, YOURS.
… Next, they assume your identity—getting a hold of your name and personal information (easy enough to do off the Internet) and using that to create fake IDs, social security cards, etc.
… Then, they go to an office supply store and purchase forms that transfer property.
… After forging your signature and using the fake IDs, they file these deeds with the proper authorities, and lo and behold, your house is now THEIRS.

… Or, Con artists look for a vacant house—say, a vacation home or rental property—and do a little research to find out who owns it. Then, they steal the owner's identity, go through the same process of transferring the deed, put the empty house on the market, and pocket the profits.

… Or, the fraudsters steal a house a family is still living in…find a buyer (someone, say, who is satisfied with a few online photos)…and sell the house without the family even knowing. In fact, the rightful owners continue right on paying the mortgage for a house they no longer own.

... Or, Offer to refi properties. Use stolen Ids or straw buyers to "purchase" these properties. Pocket borrowed money, do NOT pay mortgages. Home owners lose title, Banks lose loans, you win...or go to jail!
- http://www.mortgagefraudblog.com/index.php/weblog/permalink/la_fbi_comments_on_the_latest_scam/

Forged deeds in Florida

State and county officials say they're not sure whether they'll ever be able to stop con artists from using forged deeds to steal property. Most of the land was owned by people from across the nation and around the world who died years ago and whose property taxes were going unpaid.

Some deed scammers have forged signatures using dead owners and fake witnesses and have hijacked the stamps and seals of notaries who say they had no idea what was going on. [..] At least two notaries in Belgium said their signatures and seals were forged on deeds filed in Lee County by USA Real Estate Solutions Inc. of Punta Gorda.

Scam artists apparently are finding victims — from as far away as China, Taiwan, Spain and the Congo — by using the Internet to research vacant lots with overdue property taxes.

Florida sues Singapore man, accuses him of land fraud

Florida Attorney General Charlie Crist is suing a man he says used a Marco Island address, fraud and threats to profit from hundreds of vacant lots owned by others. According to the suit, Teal used the Internet to locate his victims, who usually lived in other states and often were elderly
- News-press.com, March 19, 2007

Mortgage Fraud – Bank Of America

Nevada's attorney general against Bank of America:

The complaint charges the bank with luring families into its loan-modification program — supposedly to help them keep their homes — under false pretenses; with giving false information about the program's requirements (for example, telling them that they had to default on their mortgages before receiving a modification); with stringing families along with promises of action, then "sending foreclosure notices, scheduling auction dates, and even selling consumers' homes while they waited for decisions"; and, in general, with exploiting the program to enrich itself at those families' expense.

Recently Dana Milbank, the Washington Post columnist, wrote about his own experience: a routine mortgage refinance with Citibank somehow turned into a nightmare of misquoted rates, improper interest charges, and frozen bank accounts. And all the evidence suggests that Mr. Milbank's experience wasn't unusual.

- http://www.nytimes.com/2011/03/14/opinion/14krugman.html?_r=1

Mortgage Fraud around the US

Las Vegas couple indicted for 227 Straw purchases. 118 of 227 in foreclosure. Properties worth $ 100M, banks lose $ 15M.

HIPAA Violation + ID Theft + Mortgage Fraud trifecta
- Erica Kaprice Pollard, vocational nurse at Kaiser Permanente, steals ID of 72-year old woman. 3 other women involved in cashing out $ 165,000 of victim's equity

Insider Collusion, Mortgage Fraud
Wachovia loan officer, Mortgage broker and title attorney find attractive properties. Recruit straw buyers, fool Wachovia using false HUD-1 settlement forms. Get Wachovia funds, falsify buyer assets, apply for first mortgages. Rinse, repeat and buy $ 37M worth of condos.

Beverly Hills Fraudsters
"Two high-profile Beverly Hills real estate agents and two licensed appraisers were indicted Thursday on charges of joining in a sophisticated scheme that lenders said cost them more than $40 million in fraudulent loans for homes in some of Southern California's most expensive neighborhoods."
Lehman is suing them for $ 40M in losses.
- all from http://www.mortgagefraudblog.com

Supply Chain Risk – Menu Foods

Menu Foods revealed that a "significant customer" [Procter & Gamble] that represented 11 per cent of last year's sales decided to end its contract to purchase cuts-and-gravy products with the company.

The Mississauga-based company ended its tumultuous day with a loss of $1.04, closing at $3.05.

The stock is now trading at half the price it was when news of tainted pet food hit front pages across North America in March after the company said melamine-laced wheat gluten from China made its way into its product line.

- http://www.theglobeandmail.com/servlet/story/LAC.20070613.RMENU13/TPStory/Business
June 13, 2007

Supply Chain Risk – Menu Foods

Larry Klimes, Paul Lavoie and Richard Mueller filed the lawsuit in U.S. District Court on Thursday. The suit seeks to be certified as a class action on behalf of all pet owners whose animals have allegedly been made sick by food made by the company.

The lawsuit alleges Menu Foods engaged in **unlawful and deceptive business practices**, violated its warranties and breached its contracts with consumers by selling its "cuts and gravy" style wet pet foods.

http://www.canada.com/nationalpost/financialpost/story.html?id=f917841f-9d78-468c-b310-ac52ff6de562&k=93293
April 7, 2007

Fake Receipts, Chinese Style

“ More than 1 million bogus receipts worth 1.05 trillion yuan (147.3 billion U.S. dollars) were confiscated in the case. The national treasury would lose more than 75 billion yuan in tax revenue if the receipts were put into circulation, officials said.”
- http://english.people.com.cn/90001/90776/6359250.html

Good News:
Ringleader gets 16 years in jail.

Bad News:
- One of their customers claimed his company was NASDAQ listed and raised $50M from unsuspecting investors.
- How many of YOUR vendors are claiming financial health using fake receipts?
- How many of YOUR employees padded their expense accounts using fake receipts?

Fake “Chisco” gear

Chinese vendors are selling counterfeit cisco gear at aggressive prices

Per FBI Presentation
- eGlobe Solutions - $ 788,000 in counterfeit gear
- Todd Richard - $ 1,000,000 in counterfeit gear

Fake equipment found in:
- US Naval Academy, US Naval Air Warfare Center, US Naval Undersea Warfare Center
- Marine Corps, Air Force, US Air Base (Spangdahelm, Germany)
- Bonneville Power Administration
- General Services Administration (GSA), FAA, FBI, other agencies and universities
- Raytheon
- Lockheed Martin (who violated rules by NOT using a GSA IT Vendor)
- MortgateIT – bought from a Authorized Cisco reseller. 30 WICs faulty.

“Cisco's Brand Protection does NOT coordinate with Cisco's Government Sales”

ATM machines with default passwords

...News reports circulated about a cyber thief who strolled into a gas station in Virginia Beach, Virginia, and, with no special equipment, reprogrammed the mini ATM in the corner to think it had $5.00 bills in its dispensing tray, instead of $20.00 bills.

…

Dave Goldsmith, a computer security researcher at Matasano Security began poking around. Based on CNN's video, he identified the ATM as a Tranax Mini Bank 1500 series. [he also found manuals for Triton and another vendor – approx 250,000 ATMs]

…

He then set out to see if he could get a copy of the manual for the apparently-vulnerable machine to find out how the hack worked. Fifteen minutes later, he reported success....[he found]

* Instructions on how to enter the diagnostic mode.
* Default passwords
* Default Combinations For the Safe

- Wired.com, September 20, 2006

Thieves steal $ 700K via POS/PIN-pad hacking

Cyber-thieves who hacked into the [debit card] information of at least 800 retail customers in California and Oregon have stolen as much as $700,000 from personal accounts during the last two months, according to police reports.

People who used [debit] cards to purchase items at Dollar Tree, a national retail toy store chain, in Modesto and Carmichael, Calif., and Ashland, Ore., have turned in reports of unauthorized withdrawals in the computer-based scam.
...
Local police said that more than 600 accounts were drained of approximately $500,000, according to the report.

- eWeek.com Aug 4, 2006

TJX (TJ Maxx, Winners, HomeSense) Breach

TJ Maxx Parent Company Data Theft Is the Worst Ever

Courtesy of Information Week

MARCH 29, 2007 | TJX Co., the parent company of T.J. Maxx and other retailers, on Wednesday dropped a bombshell in its ongoing investigation of a customer data breach by announcing in an Securities and Exchange Commission filing that more than 45 million credit and debit card numbers have been stolen from its IT systems. Information contained in the filing reveals a company that had taken some measures over the past few years to protect customer data through obfuscation and encryption. But TJX didn't apply these policies uniformly across its IT systems and as a result still has no idea of the extent of the damage caused by the data breach.

- http://www.darkreading.com/document.asp?doc_id=120810

TJX (TJ Maxx, Winners, HomeSense) Breach

Information stolen from the systems of massive retailer TJX was being used fraudulently in November 2006 in an $8 million gift card scheme, one month before TJX officials said they learned of the breach, according to Florida law enforcement officials.

...

Florida officials said the group used the increasingly common tactic of using the bogus credit cards to purchase gift cards and then cashing them at Wal-Mart and Sam's Club stores. The group usually purchased $400 gift cards because when the gift cards were valued at $500 or more, they were required to go to customer service and show identification, Pape said.

- eWeek.com March 21, 2007

Arkansas Carpenters Pension Fund, which owns 4,500 shares of TJX stock, said the company rebuffed its request to see documents detailing the safeguards on the company's computer systems and how the company responded to the theft of customer data.

The suit was filed Monday afternoon in Delaware's Court of Chancery, under a law that allows shareholders to sue to get access to corporate documents for certain purposes.

Court papers state the Arkansas pension fund wants the records to see whether TJX's board has been doing its job properly in overseeing the company's handling of customer data.

- Forbes.com, March 20, 2007

Privacy Breach – BJ's Wholesale Club

- "According to the FTC, BJ's failed to encrypt customer data when transmitted or stored on BJ's computers, kept that data in files accessible using default passwords, and ran insecure, insufficiently monitored wireless networks.
- ...**affected financial institutions filed suit against BJ's to recover damages.** According to a May securities and Exchange Commission filing, BJ's **recorded charges of $7 million in 2004 and an additional $3 million in 2005 to cover legal costs.**
- Under terms of the settlement, BJ's will implement a comprehensive information-security program subject to **third-party audits every other year for the next two decades.**
- "
- - InformationWeek 6/16/2005

Privacy Breach - DSW

- "Shoe retailer DSW Inc. agreed to beef up its computer security to settle U.S. charges that it **didn't adequately protect customers' credit cards and checking accounts,...**
- The FTC said the company **engaged in an unfair business practice** because it created unnecessary risks by **storing customer information in an unencrypted manner without adequate protection.**....
- As part of the settlement, **DSW** set up a comprehensive data-security program and **will undergo audits every two years for the next 20 years.** "
- - ComputerWorld.com 12/1/2005

- According to DSW's SEC filings, as of July 2005, the **company's exposure for losses** related to the breach ranges **from $6.5 million to $9.5 million**.
- This is the FTC's seventh case challenging faulty data security practices by retailers and others. - www.ftc.gov 12/1/2005

Privacy Breach - Choicepoint

• “The **$10 million fine** imposed today by the Federal Trade Commission on data aggregator ChoicePoint Inc. for a data security breach is yet another indication of the increasingly tough stance the agency is taking on companies that fail to adequately protect sensitive data, legal experts said.

•And it's not just companies that suffer data breaches that should be concerned. **Those companies that are unable to demonstrate duehttp://www.privacyrights.org/ar/ChronDataBreaches.htm diligence when it comes to information security practices could also wind up in the FTC’s crosshairs,** they added.

• ChoicePoint will pay a fine of $10 million...

• In addition to the penalty, the largest ever levied by the FTC, ChoicePoint has been asked to **set up a $5 million trust fund for individuals**...

• ChoicePoint will also have to **submit to comprehensive security audits every two years through 2026**. “

- ComputerWorld.com 01/26/2006

UPDATE: 12/6/06: FTC announced that victims of identity theft as a result of the data breach who had out-of-pocket expenses can now be reimbursed. The claims deadline was Feb. 4, 2007.

Click Fraud

[Stuart Cauff, CEO JetNetwork] discovered that up to "40 percent, maybe more" of the clicks on his keyword ads apparently came not from potential customers around the nation but from a single Internet address, one that belonged to a rival based in New York City. "If we get clicked fraudulently, it uses up our ad budget,".

Boris Elpiner noticed something odd about the Web traffic coming to his company from its PPC ads. As vice president of marketing for RingCentral, an online telecommunications firm in San Mateo, California, Elpiner is in charge of its affiliate-ad program, which hired Yahoo! to distribute RingCentral's ads onto Web sites with compatible content. Poring over his records, he discovered that a keyword term ("fax software download") that had previously generated almost no clicks was suddenly pulling them in. The total cost to RingCentral for the clicks - $2,500 over about four weeks - "was significant, but not immediately noticeable."
- http://www.wired.com/wired/archive/14.01/fraud.html

Click Fraud

Click fraud is perpetrated in both automated and human ways. The most common method is the use of online robots, or "bots," programmed to click on advertisers' links that are displayed on Web sites or listed in search queries. A growing alternative employs low-cost workers who are hired in China, India and other countries to click on text links and other ads. A third form of fraud takes place when employees of companies click on rivals' ads to deplete their marketing budgets and skew search results.
- http://news.com.com/Exposing+click+fraud/2100-1024_3-5273078.html

...one common scheme, he said a legitimate site is duplicated under another name, complete with text ads from a search network. A bot would then be trained to click on the ad links that appear on the bogus site, said de Souza, who estimated that click fraud affects 10 percent to 20 percent of today's search network ads.

- http://news.com.com/Exposing+click+fraud/2100-1024_3-5273078.html

Click Fraud – Do it in 3 easy steps

Firefox + Morning Coffee + Blogger.com

The process involves setting up a Blogger account and posting random crap to it. You then monetize the shit stream with Google's pay-per-click advertising program, Adsense. You then join a group of other fraudsters with equally lame blogs and add their hundreds of blogs to your Morning Coffee plugin. Then you open Morning Coffee (basically an RSS browser) and pull hits on all of these blogs every day. Your fraudster buddies do the same, all the while commenting on your lame post while you comment on theirs.
The result? Everyone gets lots of organic-looking traffic, and everyone gets paid by Adsense. Brilliant.

- http://fuzzybuzz.wordpress.com/2010/10/27/the-4chanblogger-clickfraud-circle-of-trust/

Click Fraud – Let your SMARTPHONE do it for us

ADRD appears to be targeting users on a specific Chinese website offering Android and Symbian software. This time the application hides inside legitimate wallpaper apps before setting itself up to monitor network traffic (mobile and possibly Wi-Fi), even setting alarms to wake itself at set intervals.
After sending the phone and SIM IMEI/IMSI numbers back to the attackers, the malware receives a list of web servers to hit with data traffic. This reveals its ultimate purpose – click fraud. The negative effect for an infected user would be an increased and possibly expensive level of data traffic.

- http://news.techworld.com/security/3261189/new-android-clickfraud-trojan-spotted-in-wild/

Barings, Societe Generale

- **1995 Barings Bank: $ 1.4B losses**
- **2008 Societe Generale: $ 7.1B**
- “Nick Leeson, [...] said Thursday that a massive fraud by a Société Générale employee showed that **banks still do not have risk-management controls in place**.
- "The first thing that shocked me was not necessarily that it had happened again. **I think rogue trading is probably a daily occurrence among the financial markets,**" Leeson told the British Broadcasting Corp.
- [...] "**What they're looking for is profit, profit now, and that tends to be where the money is directed**," said Leeson”
- - International Herald Tribune, http://www.iht.com/articles/2008/01/24/business/leeson.php

- “An internal investigation into billions of euros of losses at Societe Generale has found that controls at the French bank "lacked depth".
- The results of the investigation also show that rogue trades were first made back in 2005.
- - http://news.bbc.co.uk/2/hi/business/7255685.stm

Walgreens To Pay $35M To Settle Drug-Fraud Suit

CHICAGO (STNG) — Deerfield-based Walgreens will pay $35 million to settle Medicaid prescription drug-fraud claims initiated by a whistleblower, federal and state officials announced Wednesday.

The United States, 42 states and Puerto Rico will receive $35 million from Walgreen Co., which allegedly substituted different versions of prescribed drugs (such as tablets for capsules) solely to increase the cost and profit rather than for any legitimate medical reason, according to a release from the U.S. Attorney's office.

Hannaford Ruling

•**March 2008:**

• Attackers installed custom malware (spyware) to capture data in motion across Hannaford's network

• Hundreds of servers and POS terminals compromised

• 4.2 million records breached – Credit AND Debit cards

• Customers filed class-action lawsuits

May 13, 2009 ruling:

"U.S. District Court Judge Brock Hornby threw out the civil claims against the grocer for its alleged failure to protect card holder data and to notify customers of the breach in a timely fashion. In dismissing the claims, Hornby ruled that without any actual and substantial loss of money or property, consumers could not seek damages.

The only complaint he allowed to stand was from a woman who said she had not been reimbursed by her bank for fraudulent charges on her bank account following the Hannaford breach.

In a 39-page opinion, Hornby wrote that consumers with no fraudulent charges posted to their accounts could not seek damages under Maine law; neither could those who might have had fraudulent charges on their accounts that were later reversed."

-
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9133075&taxonomyId=17&intsrc=kc_top

Payment-chain supply-side risks

- 2008: Malware and/or break-ins compromise 100 million+ records at Heartland Payment Systems.
- Jan 2009: Inauguration day – Heartland discloses breach
- May 2009: Heartland has spent $ 12.6 million (and counting) in dealing with the breach.

- Feb 2009: Angie's list notices 200% increase in auto-billing transactions being declined. Autp-billing declines increased from 2% to 4%.
- May cost them $ 1 million in lost revenues so far.

- “The trouble is that convincing customers who had once set up auto-billing to reestablish that relationship after such a disruption is tricky, as many people simply don't respond well to companies phoning or e-mailing them asking for credit card information”
- - http://voices.washingtonpost.com/securityfix/2009/05/heartland_breach_dings_members.html?wprss=securityfix

Risks of Web2.0 and multi-site APIs

- **MySpace, Yahoo blame bad APIs for celebrity photos breach**
- **Paris Hilton and Lindsay Lohan's private MySpace photos are all over the Internet now, thanks to a glitch in the bad APIs.**
- http://valleywag.com/5012541/how-a-canadian-computer-guy-got-paris-hilton-and-lindsay-lohans-pics **Byron Ng's instructions for viewing any MySpace profile:**
- **1. you'll need a Yahoo account. go to www.yahoomail.com and create a yahoo account if you don't have one already. and you will need to go to www.myspace.com to sign up for a myspace account first, if you don't have one already.**
- **2.go to http://beta.m.yahoo.com/w/gallery/widget click on the 'mail' button under "sign in to yahoo!"**
- **3. click on 'click here to sign in'**
- **4. enter your yahoo id, yahoo password**
- **5. then on the top of the screen in the white box, enter: myspace then click Search Widgets Gallery**
- **6. you will see a green box in the middle with the word 'myspace' in there.**
- **7. click the green myspace.**
- **8. see in the middle of the screen it says "add it" - click that.**
- **9. click yes when it asks you about sharing info**
- **10. go here http://beta.m.yahoo.com/w/gallery/widget**
- **11. enter myspace into the box. click search widgets gallery**
- **12. click on the green myspace. now, since you have already set it up in the previous steps, it won't ask you to download again**
- **13. click on 'go to widget' (that's right below the 'already added it" text**
- **14. now sign in to myspace**
- **15. now take the URL I asked you to save above before step 1: http://beta.m.yahoo.com/w/myspace/profile/en.osl?userID=16527727 and click on it. it may ask you to sign into yahoo or my space. sign in as appropriate. now you should be able to see the person's pictures. if you can only see your own profile, then click on it again http://beta.m.yahoo.com/w/myspace/profile/en.osl?userID=16527727 then it will work.**

OpenSocial hacked within 45 minutes

- **Nov 2, 2007 – hacker compromises Plaxo's Rockyou Opensocial application.**

- **Adds 4 emoticons to reporter's account.**
- **Adds emoticon to Plaxo's VP of Marketing John McCrea's profile.**

- **Same hacker accessed any users's Facebook SuperPoke feed.**

- **- http://www.techcrunch.com/2007/11/02/first-opensocial-application-hacked-within-45-minutes/**

Facebook of the nation...

- **Facebook allows developers access to user's full profile.**
- **Every time you choose to add an application, Facebook asks you to confirm that you want to let this program both know who you are and access your information. It's impossible for anyone to add any application without agreeing to this set of terms. Once you click okay, that application can technically access quit a bit of public and private profile information.**

- **While all of the most private information (like your passwords and e-mail addresses) are kept on Facebook servers and require security authentication, a lot of info is available to applications you add.**

- **According to Facebook's Developers Terms of Use, this can include**
- **". . . your name, your profile picture, your birthday, your hometown location, your current location, your political views, your activities, your interests, your relationship status, your dating interests, your relationship interests, your summer plans, your Facebook user network affiliations, your education history, your work history, copies of photos in your Facebook Site photo albums, and a list of user IDs mapped to your Facebook friends."**
- **- http://www.removeadware.com.au/articles/facebook-privacy-hackers/**

Facebook your country's security away...



- **Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net**
- **“ MI6 faced calls for an inquiry last night after an extraordinary lapse of judgment led to the new head of MI6's personal detailsbeing plastered over Facebook.**
- **Millions of people could have gained access to compromising photographs of Sir John Sawers and his family on the social networking website. ...“**
- **http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html**



41% of Facebook users willing to divulge info to Strangers

In an experiment, 41% of Facebook users were willing to divulge highly personal information to a complete stranger. This according to IT security firm Sophos, which invited 200 randomly selected Facebookers to befriend a bogus Facebook user named “Freddi Staur” (an anagram of “ID Fraudster”). Of those queried, 87 responded to the invitation, among them 82 people whose profiles included personal information such as their email address, date of birth, address or phone number. In total:

- 72% of respondents divulged one or more email address
- 84% listed their full date of birth
- 87% provided details about their education or workplace
- 78% listed their current address or location
- 23% listed their current phone number
- 26% provided their instant-messaging screen name

Yikes. You’d think institutional privacy concerns would be enough to make folks think twice about expanding their Facebook networks with reckless gusto, wouldn’t you? Guess not.

- http://digitaldaily.allthingsd.com/20070814/facebook-privacy/

Cultural Drivers

- The Cali cartel is the wealthiest criminal organization in the history of the world, with a net worth estimated by the US government to be $206 billion-larger than almost all multinational corporations (including Exxon and Shell).
- Money laundering is the biggest business in the world. More than $1 trillion in illegal earnings are laundered annually.
- 5 Richest Criminals in History
- 1. Pablo Emilio Escobar 1949-1993 9 Billion USD (Medellin)
- 2. Carlos Lehder 1950-? 2.7 Billion USD (Medellin)
- 3. Susumu Ishii 1924-1991 1.5 Billion USD (Yakuza)
- 4.Anthony Salerno 1911-1992 600 Million USD (NYC)
- 5.Meyer Lansky 1902-1993 400 Million USD (NYC)

Cultural Drivers

- The Camorra is thought to make $70 billion a year, much of it from drugs, contraband cigarettes, and DVDs, as well as public sector contracts in construction and cleaning. Another Italian group, the 'Ndrangheta, traffics 80 percent of Europe's cocaine. The Mafia is so pervasive in Italy that, according to a large trade association, it controls one out of every five businesses in the country.

- June 3, 2008 Slate.com “Why the Mafia Loves Garbage”

Forget wine—California's biggest crop is bright green and funny-smelling - Oct 18, 2007 Economist “Home-grown”

We Make it Easy (to commit crimes)

- Criminals have existed as long as society has. And they always will.
- However, we as IT/Security/Business/Government professionals make it easy for them to commit crimes:
- **- “It's not MY problem syndrome”**
- - Bank Of America ID Theft, UK Banking rules, No liability for software vendors
- - Burden for compromise is on the victims (ID theft, house theft, spyware)
- **- The selfish gene**
- - Sony DRM rootkit, RIAA lawsuits, expired DRM
- **- Stupid IT tricks (sorry Dave)**
- - Shipping with default passwords
- - Textbooks, documentation showing insecure or poor coding practices
- **- Poor Privacy/Security planning**
- - ID theft is a growing problem today, because no one thought about limiting scope of SSN usage in 1934
- - What do Facebook, MySpace, Gmail teach our kids about privacy?
- - Are you looking at security and privacy in a holistic, global manner?

State Of Security in a nutshell





A look at how Las Vegas slots and electronic voting machines compare:

	LAS VEGAS SLOTS	ELECTRONIC VOTING MACHINES
Software	State of Nevada has access to all software. Illegal to use software that is not on file.	Software is a trade secret.
Spot-Checking	State gaming inspectors show up unannounced at casinos to compare computer chips with those on file. If there is a discrepancy, the machine is shut down and investigated.	No checks are required. Election officials have no chip to compare with the one found in the machine.
Background Scrutiny	Manufacturers subjected to background checks. Employees are investigated for criminal records.	Citizens have no way of knowing, for example, whether programmers have been convicted of fraud.
Equipment Certification	By a public agency at arm's length from manufacturers. Public questions invited.	By for-profit companies chosen and paid by the manufacturers. No public information on how the testing is done.
Handling Disputes	Casino must contact the Gaming Control Board, which has investigators on call round the clock. They can open up machines to inspect internal mechanisms and records of recent gambling outcomes.	In most cases, a voter's only recourse is to call a number at the board of elections that may or may not work to lodge a complaint that may or may not be investigated.

Success Stories

Getting it Right

Medical marijuana advocates estimate that the aggregate annual sales tax revenue that's paid by the approximately 400 dispensaries in California is $100 million.

- http://www.npr.org/templates/story/story.php?storyId=89349791

Cost of War on Drugs in 2010 (so far):

$ 23 Billion (and counting)

- http://www.drugsense.org/wodclock.htm

What was your overall IT spending last year? How much on questionable security products?

Getting it Right

"Anesthesiologists pay less for malpractice insurance today, in constant dollars, than they did 20 years ago.

That's mainly because some anesthesiologists chose a path many doctors in other specialties did not. Rather than pushing for laws that would protect them against patient lawsuits, these anesthesiologists focused on improving patient safety.
Their theory: Less harm to patients would mean fewer lawsuits. "

- Deaths dropped from 1 / 5,000 to 1 / 200,000 – 300,000
- Malpractice claims dropped 46% (from $ 332,280 in 1970 to $ 179,010 in 1990's!

Premiums dropped 37% from $ 36,620 to $ 20,572.

- http://online.wsj.com/article/0,,SB111931728319164845,00.html?mod=home%5Fpage%5Fone%5Fus

Air Force demanded, and purchased, SECURE Desktops

2006 – After years of attacks, and dealing with a hodge-podge of desktop and server configurations, The US Air Force develops the ***Secure Desktop Configuration*** standard. All vendors are required to sell computers to the USAF (and later DOD, other government agencies) with standardized, locked down configurations of:

- Windows
- MS Office
- Adobe Reader
- Norton AV
- Etc

US Dept Of Energy requires Oracle to deliver it's databases in a secure configuration developed by the **Center for Internet Security (www.cisecurity.org)**

ISO 8583 – ATM Standards

1987 Version

1993 Version

2003 Version

Each organization maps their data to the standard when communicating with other firms.

Where's the Industry standard for *SECURE INTERNAL DESKTOP CONFIGURATION? SECURE CLIENT CONFIGURATION?*

Conficker Working Group

Dec 2008 – Conficker Released.
Feb 12, 2009 – Microsoft offers $ 250,000 reward for identifying authors
Mar 31, 2009 – Nmap, Nessus, other tools release conficker detection tools

Current Status: Conficker practically eradicated (just like SmallPox)

However, Zeus and other bots are using what they learned from Conficker.

Microsoft – Security Champion!

Microsoft to assume control of Waledac domains
http://www.scmagazineus.com/microsoft-to-assume-control-over-waledac-domains/article/178492/

Microsoft sues hotmail domain squatters (ho0tmail, hot5mail, etc)
http://blog.seattlepi.com/microsoft/archives/198358.asp

Microsoft sues fake Antivirus peddlers
http://www.darkreading.com/security/antivirus/showArticle.jhtml?articleID=220100423

Microsoft sues spammers who abused it's spam filters
http://www.esecurityplanet.com/news/article.php/3888571/Microsoft-Sues-Spammers-Who-Abused-Its-Spam-Filters.htm

Microsoft Security Essentials – Free AV software that works **exceptionally well**
http://www.microsoft.com/security_essentials/

Shameless Self-promo

Brainlink provides COMMON SENSE BASED IT Security and Privacy Breach law compliance audits

We can help YOU address your CIO / CPO / CFO intelligently, with relevant data and proper presentation materials

Information Security Audits (PCI, HIPAA, Privacy Breach)
IT Consulting for Healthcare

If you like what you're hearing, hire us!

www.brainlink.com

Contact Information

Raj Goel, CISSP

Chief Technology Officer

Brainlink International, Inc.

C: 917-685-7731

raj@brainlink.com

www.brainlink.com

www.linkedin.com/in/rajgoel



Questions?

Click on the questions tab on your screen, type in your question, name and e-mail address; then hit submit.

