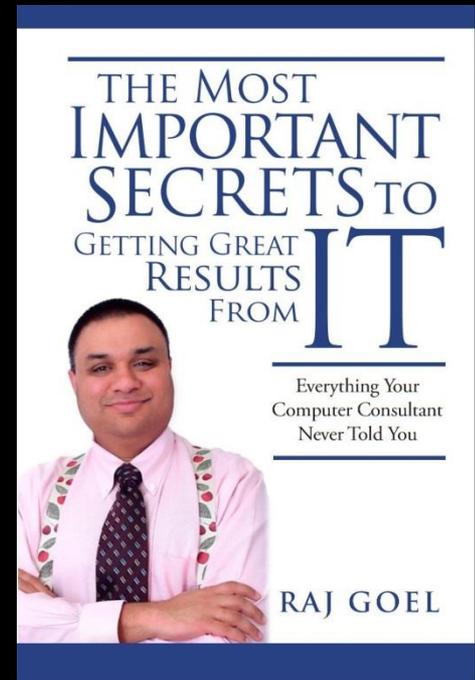


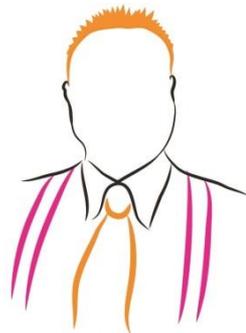
# Trends In Financial Crimes

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



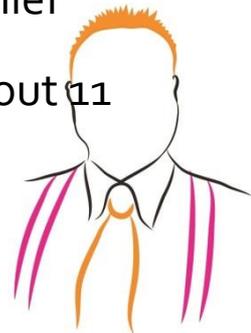
# Agenda

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



# 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



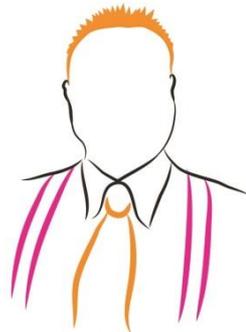
# Economics of SPAM

- 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," Alperovitch said. [...]that is up from over 70 percent a year ago.
- - eWeek, March 11, 2007



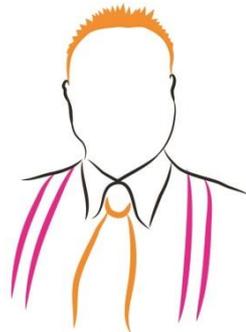
# Priceline, Travelocity, and Cingular fined for using adware

- 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



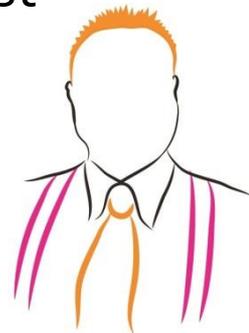
# Spyware - Israel's TrojanGate

- “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/>



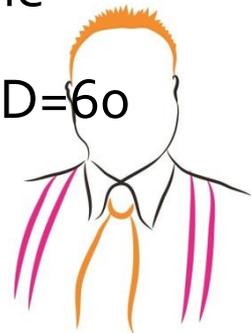
# Spyware - Japan's Winny P2P

- “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 is the first known case of a business customer of a U.S. bank claiming to have suffered a loss as a result of a hacking incident.
- 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>



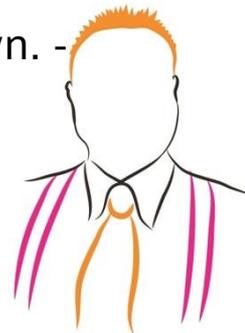
# Spyware - Sony's DRM Rootkit

- 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

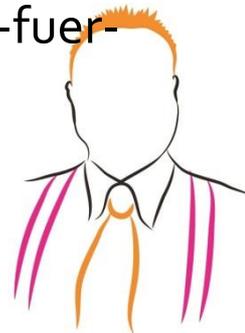
- Oct 31, 2005 - Mark Russinovich, a security researcher, discovers that Sony's CDs install a rootkit
- Nov 3 – Sony releases rootkit remover. Ed Felten dismisses the rootkit remove as junk
- Sony's rootkit used to defeat World of Warcraft's security
- Nov 15 – Sony's rootkit uninstaller “create huge 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](http://sonysuit.com)



# Spyware - Sony's DRM Rootkit

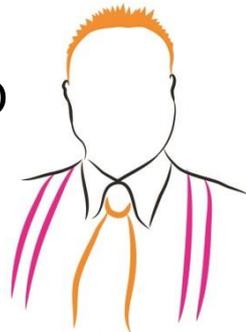
## Anastacia CD costs retailer 1,500 Euros

- 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-Schadenersatz-fuer-Sony-Rootkit-CD-zahlen--/meldung/145233>



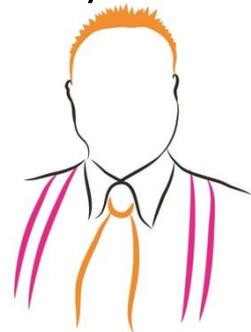
# ID Theft – Bank Of America & Margaret Harrison

- 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"



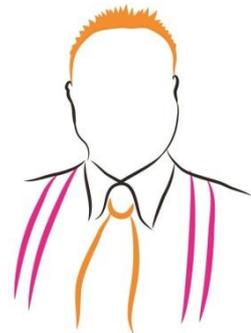
# Walmart Mexico Bribery Case

- Vast Mexico Bribery Case Hushed Up by Wal-Mart After Top-Level Struggle
- Confronted with evidence of widespread corruption in Mexico, top Wal-Mart executives focused more on damage control than on rooting out wrongdoing, an examination by The New York Times found.
- NY Times April 21, 2012
- <http://www.nytimes.com/2012/04/22/business/at-wal-mart-in-mexico-a-bribe-inquiry-silenced.html>
- The payments at issue are comparatively paltry, perhaps totaling less than \$50 million, although that number could increase as the internal investigation moves forward. The ultimate cost to Wal-Mart for the legal and accounting fees for the investigation, along with any monetary penalties the Justice Department and the S.E.C. may seek, will probably far exceed the bribes.
- NY Times, April 23, 2012



# Walmart Mexico Bribery Case – Michaels Impact

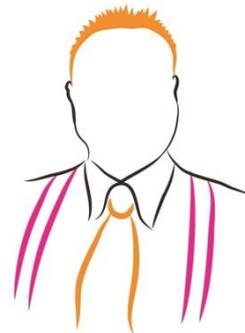
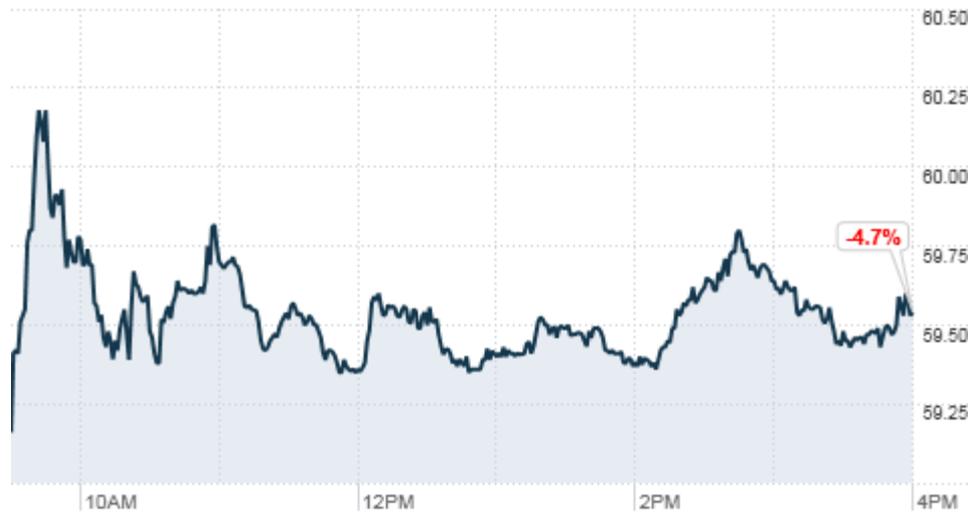
- Michaels Stores C.E.O. Connected to Wal-Mart Bribery Case
- Mr. Menzer joined Michaels in March 2009 after serving as vice chairman and chief administrative officer of Wal-Mart. The Times story reported that in the fall of 2005, Mr. Menzer intervened in an internal investigation into a senior vice president who reported to him.
- According to internal records, Mr. Menzer told an investigator that he did not want Wal-Mart's corporate investigations unit to handle the inquiry because of concerns about the impact such an investigation would have, the story said. Mr. Menzer suggested that one of the senior vice president's subordinates was better suited to handle the inquiry, according to the article.
- "Soon after, records show, the subordinate cleared his boss," the story said.
- NY Times April 23, 2012
- <http://dealbook.nytimes.com/2012/04/23/michaels-stores-c-e-o-implicated-in-wal-mart-bribery-case/>



# Walmart Stop drops 4.7%

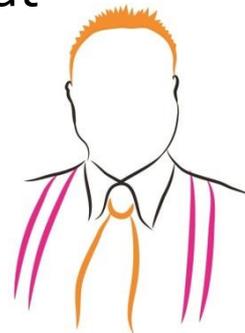
- [http://money.cnn.com/2012/04/23/markets/walmart\\_stock/index.htm](http://money.cnn.com/2012/04/23/markets/walmart_stock/index.htm)

Wal-Mart Stores



# Telemarketing Fraud

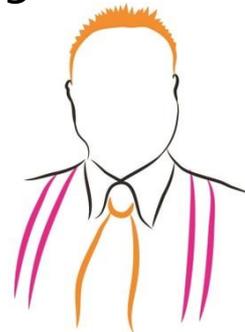
- Telemarketing fraud, predominately emanating from Canada, is a flourishing crime problem with estimated losses to U.S. elderly citizens exceeding \$500 million per year.
- - [http://www.fbi.gov/publications/financial/fcs\\_reporto52005/fcs\\_reporto52005.htm](http://www.fbi.gov/publications/financial/fcs_reporto52005/fcs_reporto52005.htm)
- 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](http://www.rcmp-grc.gc.ca/organizedcrime/octa_e.htm)



# Global Payments – 1.5MM cards stolen

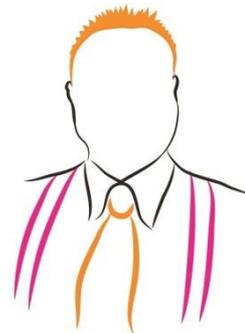


- Visa Drops Support for Breached Processor, Acknowledges Weekend Outage
- Global Payments, the credit and debit card processor that disclosed a breach of its systems late Friday, said in a statement Sunday that the incident involved at least 1.5 million accounts. The news comes hours ahead of a planned conference call with investors, and after Visa said it had pulled its seal of approval for the company.
- - <http://krebsonsecurity.com/page/2/>



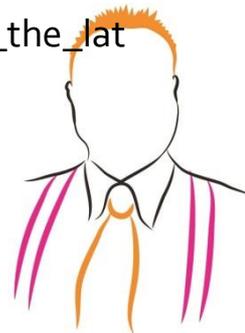
# Homeowners lose houses in property scams

- 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\\_lat\\_est\\_scam/](http://www.mortgagefraudblog.com/index.php/weblog/permalink/la_fbi_comments_on_the_lat_est_scam/)



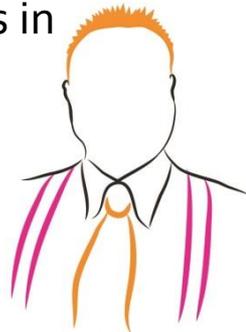
# Forged deeds in Florida

- 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



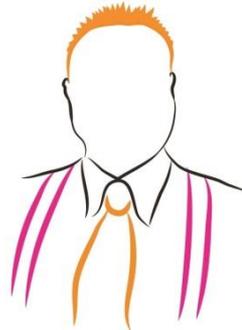
# Mortgage Fraud around the US

- 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>



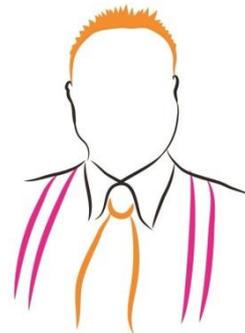
# Supply Chain Risk – Menu Foods

- 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



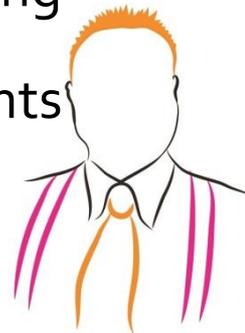
# Supply Chain Risk – Menu Foods

- 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



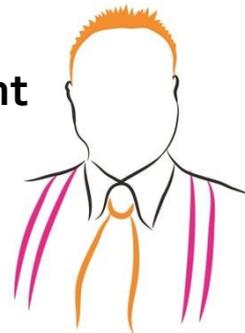
# Fake Receipts, Chinese Style

- “ 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?



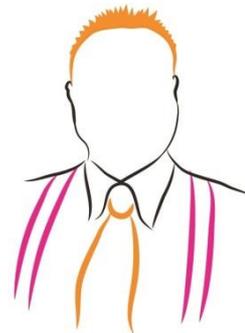
# Fake “Chisco” gear

- 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)
  - - MortgageIT – bought from a Authorized Cisco reseller. 30 WICs faulty.
- **“Cisco's Brand Protection does NOT coordinate with Cisco's Government Sales”**



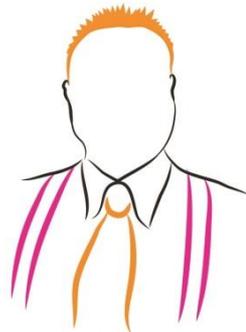
# ATM machines with default passwords

- ...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



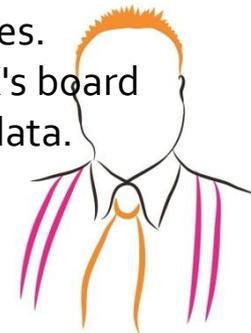
# TJX (TJ Maxx, Winners, HomeSense) Breach

- 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](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



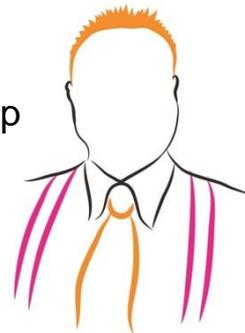
# Cost of carelessness

**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
<b>Detection &amp; Escalation</b>				
- Internal investigation	\$19,000	\$488,000	N/A	\$507,000
- Legal consulting	463,000	51,000	N/A	514,000
<b>Notification</b>				
- 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
<b>Ex-Post Response</b>				
- 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
<b>Lost Business</b>				
- Lost existing customers	N/A	N/A	6,728,000	6,728,000
- Lost new customers	N/A	N/A	730,000	730,000
<b>AVERAGE COST PER COMPANY</b>	<b>\$4,990,000</b>	<b>\$1,347,000</b>	<b>\$7,458,000</b>	<b>\$13,795,000</b>
<b>PER LOST RECORD COST</b>	<b>\$50</b>	<b>\$14</b>	<b>\$75</b>	<b>\$138</b>

SOURCE: PGP CORP.

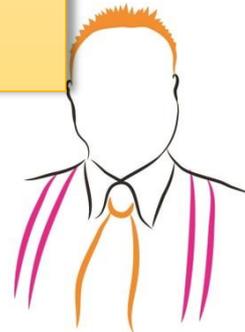
The Cost of Carelessness 12/5/2005 - <http://www.ciainsight.com/article2/0,1540,1906158,00.asp>



# The Cost of Breaches 2005-2011

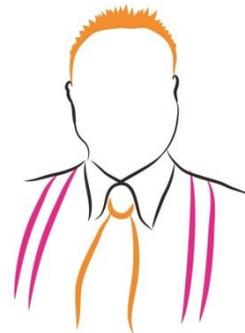
Year	Direct Costs	Indirect Costs	Costs Per Record	Total Cost Of Cleanup
2005	50	88	138	\$4.54M
2006	54	128	182	\$4.79M
2007	52	145	197	\$6.36M
2008	50	152	202	\$6.66M
2009	60	144	204	\$6.75M
2010	73	141	214	\$7.24M
2011	59	135	194	\$5.50M

Ponemon Institute 2011 Cost of Data Breach Study



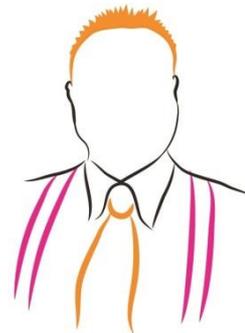
# The Cost of Breaches 2005-2011 (2)

- 1st Time Victims Cost: \$ 243/record
- Experienced victims Cost: \$ 192/record
- Churn Rates:
  - Average 3.6%
  - Healthcare 4.2% @ \$282/Record
  - Financial Services 5.6%
- 88% breaches due to insider negligence
- 44% due to external parties



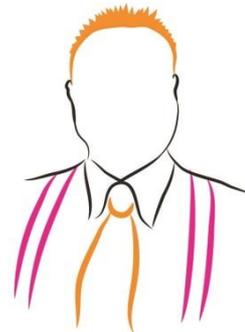
# Privacy Breach – BJ's Wholesale Club

- “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](http://www.ftc.gov) 12/1/2005



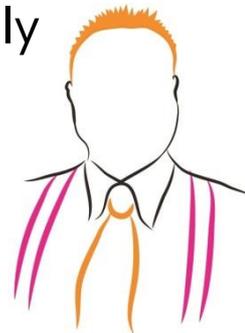
# Privacy Breach - Choicepoint

- “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 due <http://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



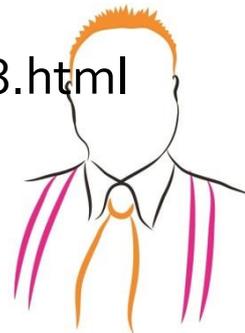
# Click Fraud

- [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>



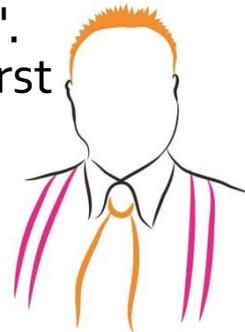
# Click Fraud

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



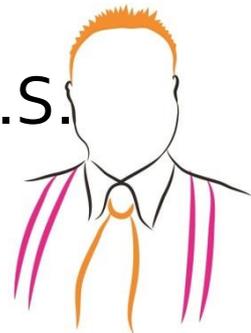
# Barings, Societe Generale

- 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>



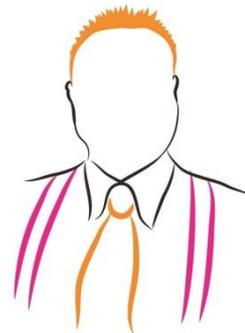
# Walgreens To Pay \$35M To Settle Drug-Fraud Suit

- 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.



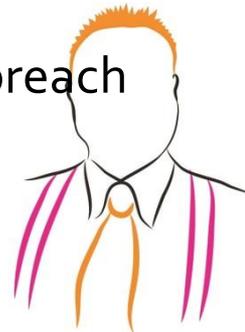
# Hannaford Ruling

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

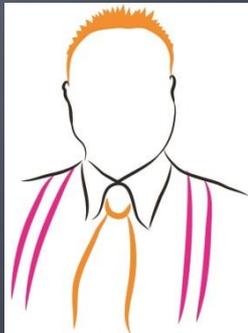


# Payment-chain supply-side risks

- 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](http://voices.washingtonpost.com/securityfix/2009/05/heartland_breach_dings_members.html?wprss=securityfix)



# Government & Vendors

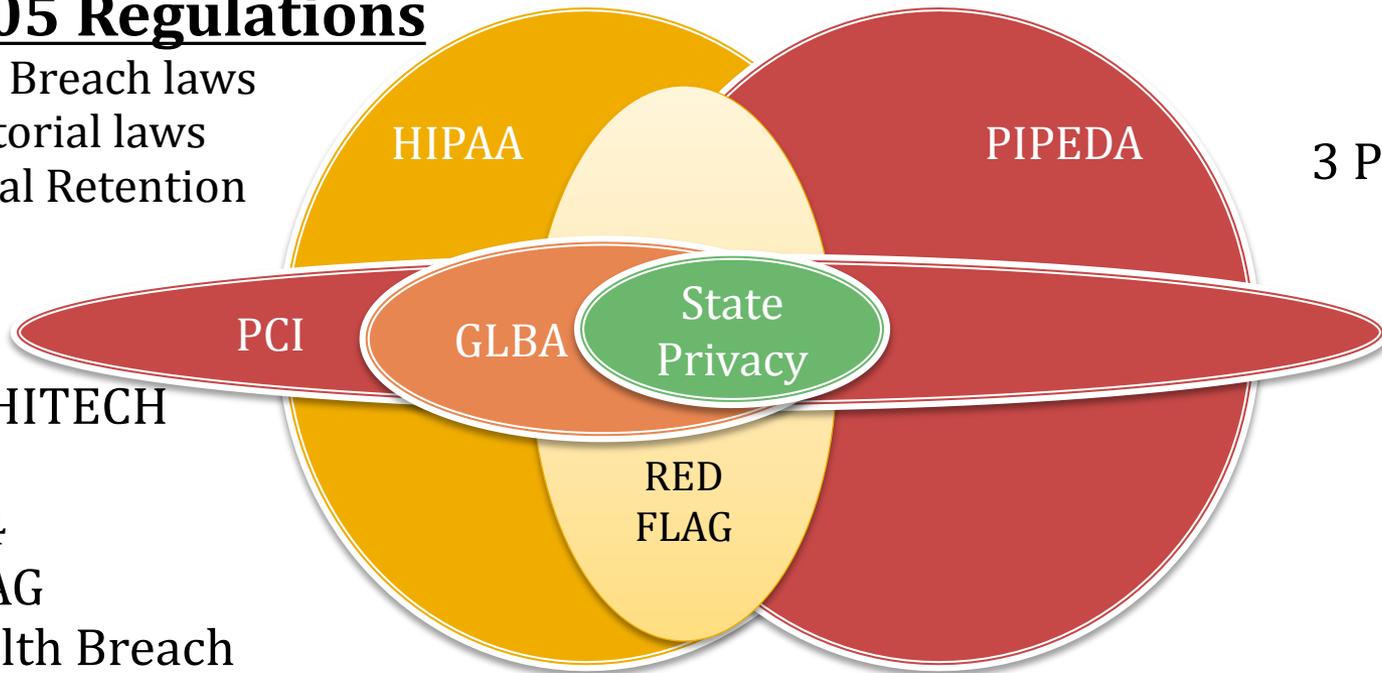


# Standards Explosion

## US – 105 Regulations

46\* State Breach laws  
3\*\* Territorial laws  
50 Medical Retention

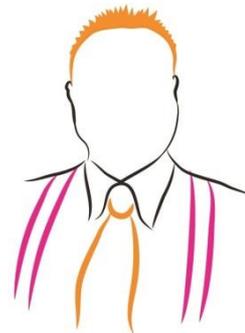
PCI  
HIPAA/HITECH  
GLBA  
SOX-404  
RED FLAG  
FTC Health Breach



## Canada

PIPEDA  
3 PIPA/PPIPS  
laws

- \*Texas State law covers the 4 states Alabama, Kentucky, New Mexico, and South Dakota
- \*\* Territories: Washington DC, Puerto Rico, US Virgin Islands



# Every Law Has Protected Fields

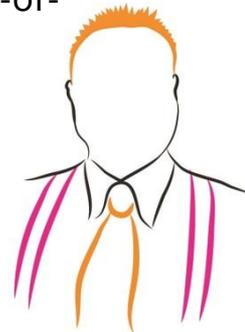
- Names
- Postal address
- Tel & fax number
- Email address
- SSN
- Medical record number
- Health plan number
- Certificate/license number
- Vehicle ID or license
- Device identifiers
- Web URLs
- Internet protocol
- Biometric ID
- Full face, comparable image

Latanya Sweeney showed that 87% of all Americans can be identified by ZIP Code, DOB, sex.



# De-Identification

- The Massachusetts Group Insurance Commission had a bright idea back in the mid-1990s—it decided to release "anonymized" data on state employees that showed every single hospital visit. The goal was to help researchers, and the state spent time removing all obvious identifiers such as name, address, and Social Security number. But a graduate student in computer science saw a chance to make a point about the limits of anonymization.
- Latanya Sweeney requested a copy of the data and went to work on her "reidentification" quest. It didn't prove difficult. Law professor Paul Ohm describes Sweeney's work:
  - At the time GIC released the data, William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers. In response, then-graduate student Sweeney started hunting for the Governor's hospital records in the GIC data. She knew that Governor Weld resided in Cambridge, Massachusetts, a city of 54,000 residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge, a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor Weld with ease. Only six people in Cambridge shared his birth date, only three of them men, and of them, only he lived in his ZIP code. In a theatrical flourish, Dr. Sweeney sent the Governor's health records (which included diagnoses and prescriptions) to his office.
- - <http://arstechnica.com/tech-policy/news/2009/09/your-secrets-live-online-in-databases-of-ruin.ars>



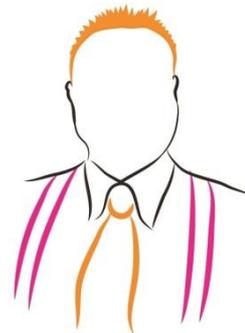
# Social Security Numbers – A Brief History

- 1936 - SSNs established
- 1938 - Wallet manufacturer includes secretary's SSN card inside a wallet. 40,000 people thought it was their SSN. 12 people used it in 1977.
- Pre-1986 - kids under 14yrs not required
- Post-1990 - Kids get SSN # with Birth Certificate
- Repeatedly, laws state that “we” oppose the creation of a national ID card. SSNs become defacto national ID numbers.
- Result: Experian, TransUnion, Equifax
- [http://en.wikipedia.org/wiki/Social\\_Security\\_number](http://en.wikipedia.org/wiki/Social_Security_number)
- <http://www.socialsecurity.gov/history/ssn/ssnchron.html>



# Social Security Numbers Fraud – Target: Kids

- The numbers are run through public databases to determine whether anyone is using them to obtain credit. If not, they are offered for sale for a few hundred to several thousand dollars.
- Because the numbers often come from young children who have no money of their own, they carry no spending history and offer a chance to open a new, unblemished line of credit. People who buy the numbers can then quickly build their credit rating in a process called "piggybacking," which involves linking to someone else's credit file.
- If they default on their payments, and the credit is withdrawn, the same people can simply buy another number and start the process again, causing a steep spiral of debt that could conceivably go on for years before creditors discover the fraud.
- <http://www.foxnews.com/us/2010/08/02/ap-impact-new-id-theft-targets-kids-social-security-numbers-threaten-credit-737395719/>



# Adobe Flash Player

Download the latest version of Adobe Reader



Adobe Reader 9.3  
(includes Acrobat.com on Adobe AIR)  
Windows XP SP2 - SP3, English

37.85 MB

[Different language or operating system?](#)

[Learn more](#) | [System Requirements](#) | [License](#) | [Distribute Adobe Reader](#)

Also install:

Free McAfee® Security Scan Plus  
(optional) 1 MB

 McAfee® | Security Scan Plus

[Check the status of your PC security.](#)

[Learn more](#) | [Privacy policy](#) | [License](#)

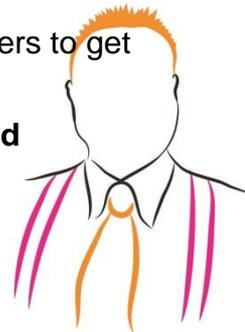
Download

Total :  
38.85 MB

## Adobe Flash is the root of Browser Insecurity

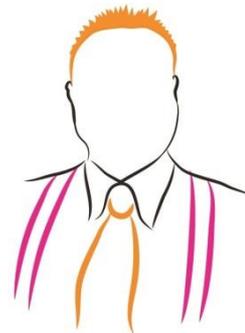
“Chrome or IE8 on Windows 7 with no Flash installed. There probably isn't enough difference between the browsers to get worked up about. The main thing is not to install Flash!”

<http://gizmodo.com/5483024/security-expert-flash-is-the-root-of-browser-insecurity-oh-and-ie8-isnt-so-bad>



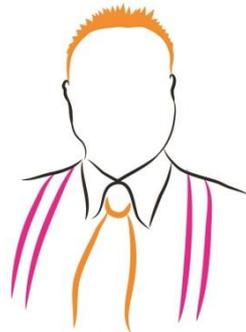
# Dell Ships infected Motherboards

- July 2010 – Dell blames “human error” for shipping thousands of infected Server motherboards – Poweredge 310, 410, 510, T410.
- [http://www.theregister.co.uk/2010/07/23/dell\\_malware\\_update/](http://www.theregister.co.uk/2010/07/23/dell_malware_update/)



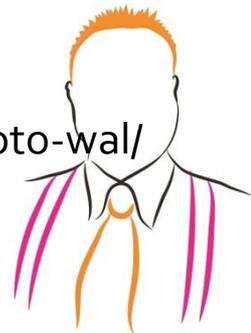
# HP ships infected keys

- April 2008 – HP ships infected keys to Enterprise Customers using Proliant servers.
- <http://www.engadget.com/2008/04/07/hp-sends-server-customers-virus-infected-usb-keys/>



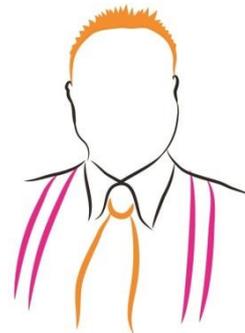
# Walmart, Amazon, etc. used as infection vectors

- Jan 2009 – Hundreds of thousands (millions?) of picture frames sold by Walmart, SamsClub, Amazon ship from the factory with embedded malware.
- NOTE: Picture frame sales
- 2007 - 5 million
- 2008 - 7.4 million
- 2009 - 9.8 million
- [http://articles.sfgate.com/2009-01-02/business/17196259\\_1\\_frames-digital-photo-wal/](http://articles.sfgate.com/2009-01-02/business/17196259_1_frames-digital-photo-wal/)



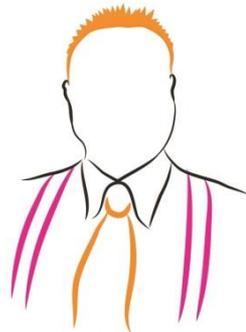
# Cultural Drivers

- Spitzer Exposed by Bank's Anti-Money Laundering Technology
- Ex-Newark mayor Sharpe James and his ex-mistress found guilty of corruption
- Antoin Rezko found guilty of 16 counts, including fraud, money laundering and bribery
- IGOR KLOPOV..Indicted for Identity Theft. Prosecutors said yesterday that Mr. Klopov was self-taught in the art of Internet identity theft and had used a combination of Internet smarts and old-fashioned techniques like forging driver's licenses, powers of attorney and funds transfer request forms, hiring private investigators and using accomplices to assume the identities of victims.



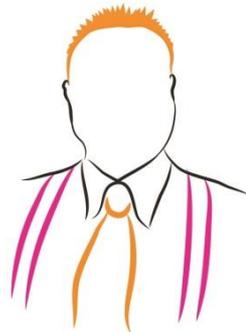
# Cultural Drivers

- 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)



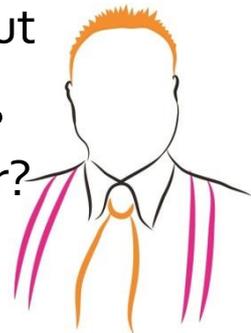
# Cultural Drivers

- 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?



# 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>



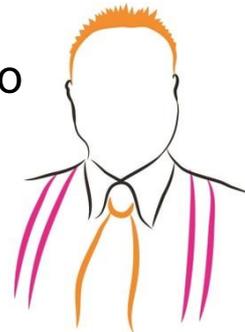
# Getting it Right

- 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 2009 (so far):
- \$ 20 Billion (and counting)
- - <http://www.drugsense.org/wodclock.htm>

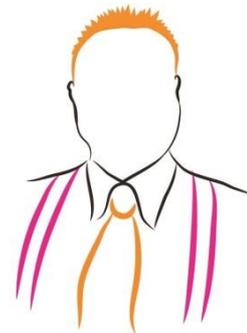
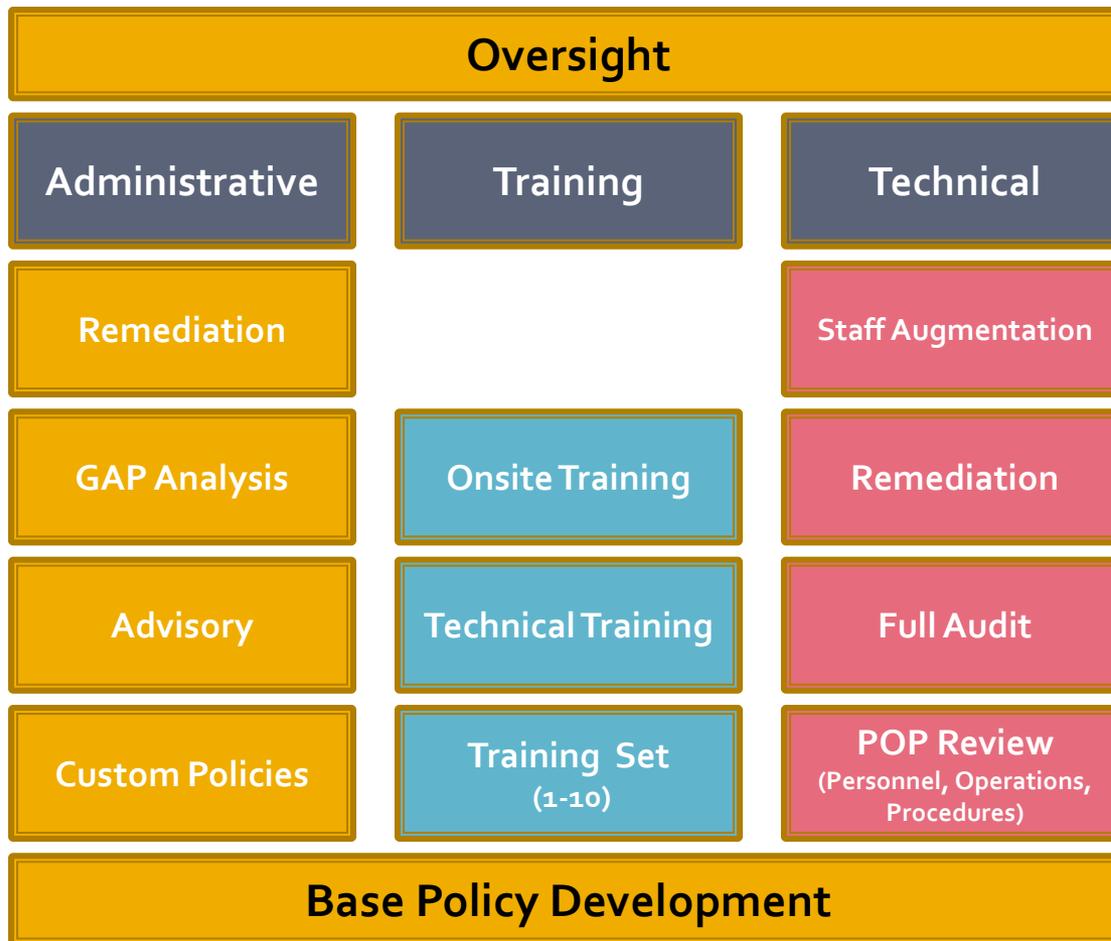


# Recommended Reading

- <http://www.rajgoel.com/infosecurity-issue-6-%e2%80%94-data-leak-googling-away-your-security-and-privacy>
- <http://www.rajgoel.com/infosecurity-issue-7-%e2%80%93-trends-in-financial-crimes-2>
- <http://www.rajgoel.com/backing-up-documents-in-the-cloud>
- <http://www.rajgoel.com/how-much-does-facebook-know-about-you-about-800-pages>
- <http://www.rajgoel.com/how-do-spammers-credit-card-thieves-spyware-creators-make-money>
- <http://www.eff.org/cases/warshak-v-usa>
- <http://blog.jayparkinsonmd.com/post/92060107/the-promise-of-google-health-and-data-liquidity-in>
- <http://google.about.com/od/experimentalgoogletools/qt/GoogleFluTrends.htm>
- <http://www.schneier.com/news-062.html>
- [http://threatpost.com/en\\_us/blogs/effect-snake-oil-security-090710](http://threatpost.com/en_us/blogs/effect-snake-oil-security-090710)

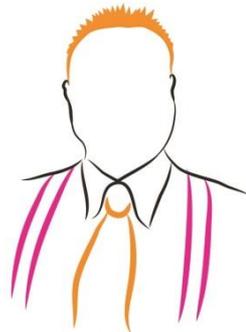


# Compliance Roadmap



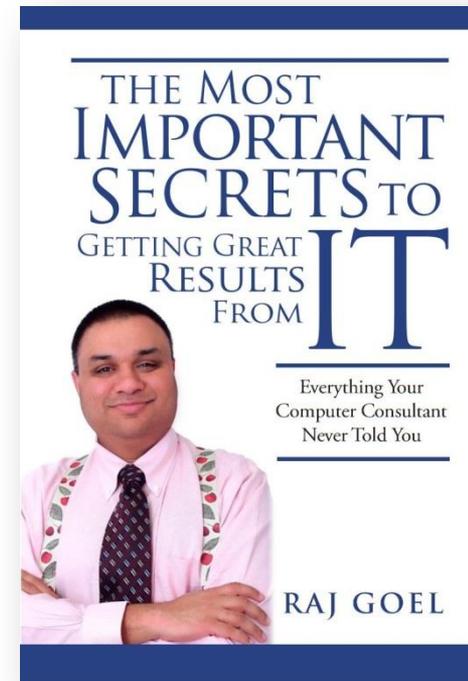
# Need Help?

[www.ITSecurityConsultant.com](http://www.ITSecurityConsultant.com)



# Contact Information

**Raj Goel, CISSP**  
Chief Technology Officer  
Brainlink International, Inc.  
C: 917-685-7731  
raj@brainlink.com  
www.RajGoel.com  
www.linkedin.com/in/rajgoel



Author of "The Most Important Secrets To Getting Great Results From IT"  
<http://www.amazon.com/gp/product/0984424814>

