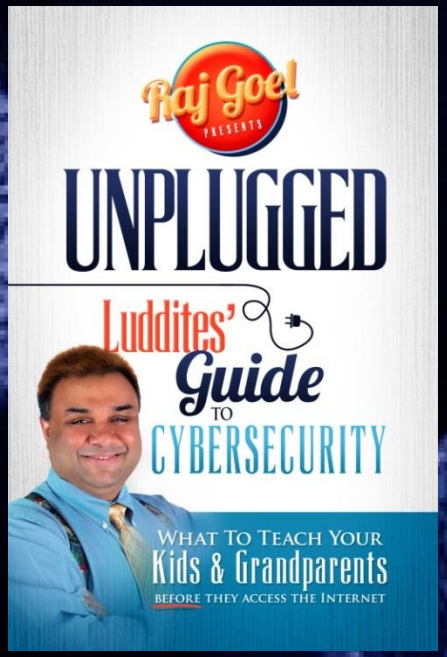
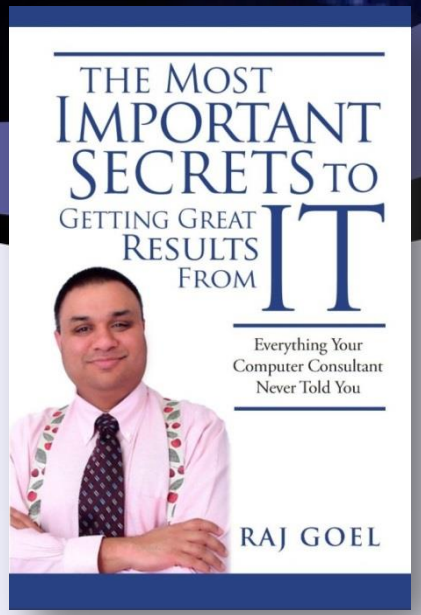
Trends In Financial Crimes - 2015

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

OWASP
The Open Web Application Security Project





Raj Goel, CISSP

OWASP
The Open Web Application Security Project

Author, entrepreneur, IT expert and public speaker, Raj Goel is globally known as the go-to man in cyber security and privacy law. He is committed to educating individuals and organizations about online safety and how to protect their most important assets – **people and data**. His expert advice helps individuals, companies and conglomerates navigate their way through the world's ever-changing technology and increasingly complex IT compliance laws. He often appears in the media and at conferences world-wide to educate the public on cyber-security and digital privacy, a subject he is passionate about.

Security, Civil Liberties and Peace of Mind

When you need the right approach to complying with HIPAA/HITECH, PCI-DSS or simply protecting your assets, Raj Goel, as any of his loyal clients will tell you, is the man to call upon. Raj's credentials are impeccable. A 25-year veteran of the IT industry and an expert in online security, Raj has personally consulted with organizations ranging from Fortune 100 corporations to small family companies to governments world wide.

Raj is fueled by his passion for enhancing Civil Rights in Cyberspace, his love of helping people keep themselves, their families and their companies safe online. He is available as a consultant and a public speaker and often sought after by major media outlets and companies.

Key highlights:

- **Author,** "UNPLUGGED Luddites Guide To Cybersecurity", **Amazon**, 2015
- **Author,** "The Most Important Secrets To Getting Great Results From IT", **Amazon**, 2012
- **On-Air Television Cybersecurity Expert**, **WPIX11**, New York City (2013-present)
- **On-Air Cybersecurity Expert**, Columbia News Tonight, **Columbia University**, NYC
- **Keynote speaker**, NCSL 2013, **Government of Netherlands**, The Hague, Netherlands
- **Keynote speaker**, **Government Of Curacao**, 2013
- **Keynote speaker**, "**what should MSP's know about compliance**", **Datto** partner conference, 2013
- **Author**, "Googling Your Privacy and Security Away", **Infosecurity Professional Magazine**
- **Author**, "Trends In Financial Crimes", **Infosecurity Professional Magazine**
- **Author**, "Life Of A Child (2014) – raising a generation of cyber-at-risk youth", **Infosecurity Professional Magazine**, 2014
- **Author**, "Welcome To The World Of Dating Sites", **Infosecurity Professional Magazine**, 2015

Media Appearances

OWASP

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

GBATA | Global Business and Technology Association™

CSO
BUSINESS RISK LEADERSHIP

ASIS INTERNATIONAL
Advancing Security Worldwide®

The New York Times

Entrepreneur

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY℠

BrightTALK™

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

FOX NEWS Channel

CyberHood Watch

PBS

DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES
OFFICE OF COUNTER TERRORISM
NEW YORK STATE

NYIT MAGAZINE

CNNfn
the financial network

PenTest magazine

ITV

NEW YORK COUNTY
NYCLA
LAWYERS' ASSOCIATION

Common Rationales

OWASP
The Open Web Application Security Project

- There's nothing a hacker would want on my PC
- I don't store sensitive information on my PC
- I only use my computer for checking email
- My firm isn't big enough to worry about hackers or cyber crime

Are You Part Of The 93%? Or 7%?

OWASP
The Open Web Application Security Project

93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately.

(Source: National Archives & Records Administration in Washington)

1 in 5. Care to place a bet?

OWASP
The Open Web Application Security Project

20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years.

(Source: Richmond House Group)

Patco Construction

OWASP
The Open Web Application Security Project

- A Maine-based construction firm got infected with the Zeus Trojan virus and $588,851.26 was transferred from their accounts. Their bank recovered $243,000 but Patco was on the hook for $345,000. Patco was dragged through three years of lawsuits by their bank before the case settled.

- **"We had hundreds of thousands of dollars in legal fees," says Patterson. "So even after we got the $345,000 back, we lost hundreds of thousands.**

New Years Eve Burgulary Shutters Billing Firm

OWASP
The Open Web Application Security Project

- Impairment Resources LLC filed for bankruptcy after the break-in at its San Diego headquarters led to the electronic escape of detailed medical information for roughly 14,000 people, according to papers filed in U.S. Bankruptcy Court in Wilmington, Del. That information included patient addresses, social security numbers and medical diagnoses.
- **Police never caught the criminals, and company executives were required by law to report the breach to state attorneys general** and the Department of Labor's Office of Inspector General. Some of those agencies, including the Department of Labor, are still investigating the matter, the company said in court papers.
- **"The cost of dealing with the breach was prohibitive"** for the company, Impairment Resources said when explaining its decision to file for Chapter 7 bankruptcy protection. That type of bankruptcy is used most often by companies to shut down and sell off what's left to pay off their debts.
- The company said its assets are worth about $226,000, an amount that, even after money trickles in from liquidating sales, likely won't be enough to pay lender Insurance Recovery Group and its $583,000 loan, Impairment Resources said in court papers.

$1.5M Cyberheist Ruins Escrow Firm

OWASP
The Open Web Application Security Project

- The heist began in December 2012 with a roughly $432,215 fraudulent wire sent from the accounts of Huntington Beach, Calif. based **Efficient Services Escrow Group** to a bank in Moscow. In January, the attackers struck again, sending two more fraudulent wires totaling $1.1 million to accounts in the Heilongjiang Province of China, a northern region in China on the border with Russia.
- When Efficient reported the incident to state regulators, the **California Department of Corporations** gave the firm three days to come up with money to replace the stolen funds.
- This forced the California escrow firm to close and lay off its entire staff.

Ex-Worker, Husband Sentenced In Pa. Law Firm Hacking

OWASP
The Open Web Application Security Project

- Law360, New York (October 18, 2013, 6:09 PM ET) -- A former employee of a Pittsburgh, Pa., law firm and her husband were each sentenced Friday to three years of probation, on federal charges that they hacked into the firm's computers in conjunction with a supposed member of the international hacker network Anonymous
- Alyson Cunningham, 25, and Jonathan Cunningham, 29, pled guilty in June to two counts of damaging a computer and unlawfully trafficking in passwords. The actions in question took place after Alyson Cunningham was fired from her job at Voelker & Gricks LLC in 2011.

China-Based Hackers Target Law Firms to Get Secret Deal Data

OWASP
The Open Web Application Security Project

- China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer **Potash Corp (Ca)** by an Australian mining giant **BHP Biliton Ltd (Aus**) zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal.
- Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, **eventually hitting seven different law firms** as well as Canada's Finance Ministry and the Treasury Board
- - Bloomberg.com

OWASP
The Open Web Application Security Project

- [former website administrator] had his servers wiped clean of all client email, not simply the Puckett firm's material.
- The firm's Google email passwords weren't secure enough to keep out hackers who may have been using equipment that can rapidly try out multiple possible combinations, according to Puckett. So the firm has changed all of its email passwords and made them more complex. Fortunately, although the email was copied by Anonymous hackers, it wasn't deleted.
- - ABA Journal

Client Secrets at Risk as Hackers Target Law Firms

OWASP
The Open Web Application Security Project

- Cyberattacks against law firms are on the rise, and that means attorneys who want to protect their clients' secrets are having to reboot their skills for the digital age.
- Lawyers sling millions of gigabytes of confidential information daily through cyberspace, conducting much of their business via email or smartphones and other mobile devices that provide ready access to documents. But the new tools also offer tempting targets for hackers, who experts say regard law firms as "soft targets" in their hunt for insider scoops on mergers, patents and other deals.
- - Wall Street Journal

Law firm's trust account hacked, 'large six figure' taken

OWASP
The Open Web Application Security Project

- A law firm lost "a large six figure" over the holidays after a virus gave hackers backdoor access to its bookkeeper's computer. The virus copied bank account passwords as she typed them.
- The virus "tricked the [bookkeeper] into giving the trust account's password to the fraudsters, allowing them essentially full access to the trust account, including the ability to go in, monitor it, and wire money to foreign countries shortly after deposits were made,"
- Lawtimes.com

Attack of the Zombie computers

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- **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

OWASP
The Open Web Application Security Project

- “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

OWASP
The Open Web Application Security Project

- “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

OWASP
The Open Web Application Security Project

- " 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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%

OWASP
The Open Web Application Security Project

- http://money.cnn.com/2012/04/23/markets/walmart_stock/index.htm

Telemarketing Fraud

OWASP
The Open Web Application Security Project

- 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

Global Payments – 1.5MM cards stolen

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- " 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- ...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

Payment-chain supply-side risks

OWASP
The Open Web Application Security Project

- 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

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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- "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

OWASP
The Open Web Application Security Project

- "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

OWASP
The Open Web Application Security Project

- "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

Click Fraud

OWASP
The Open Web Application Security Project

- [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

OWASP
The Open Web Application Security Project

- 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

Barings, Societe Generale

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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.

OWASP
The Open Web Application Security Project

Government & Vendors

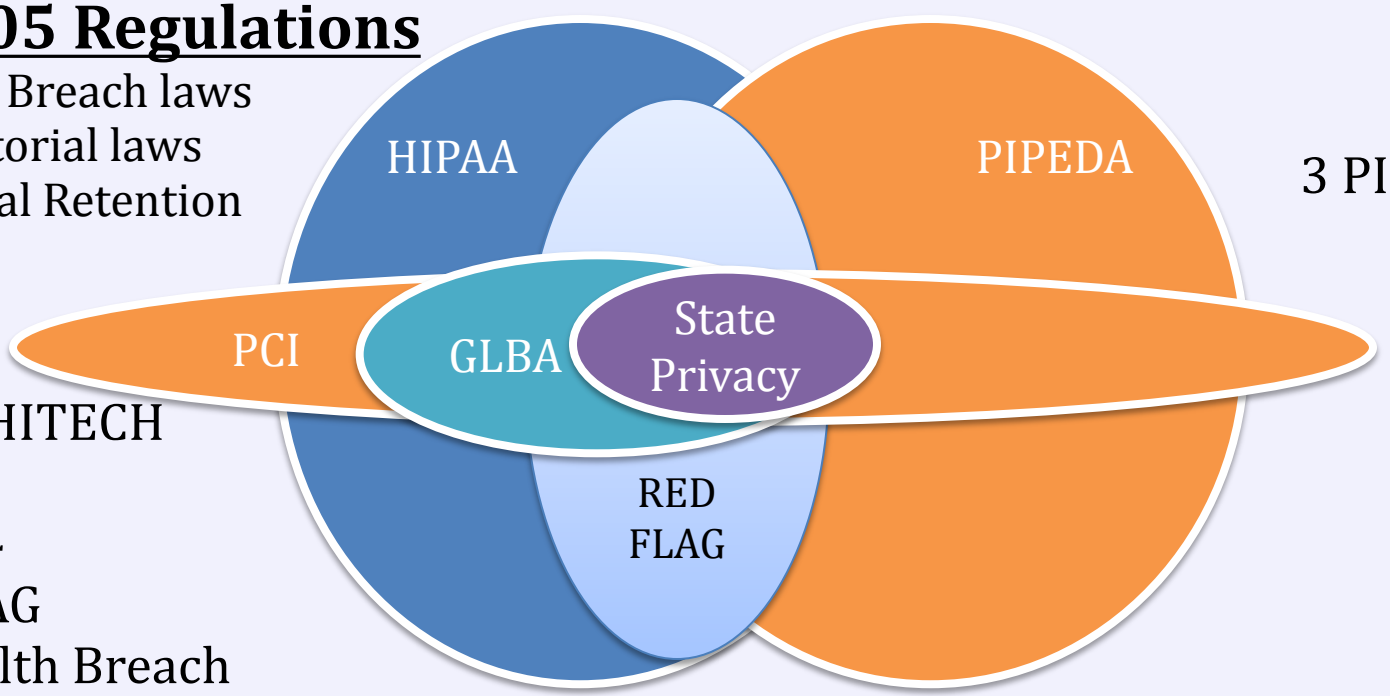
Standards Explosion

OWASP
The Open Web Application Security Project

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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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://www.socialsecurity.gov/history/ssn/ssnchron.html

Social Security Numbers Fraud – Target: Kids

OWASP
The Open Web Application Security Project

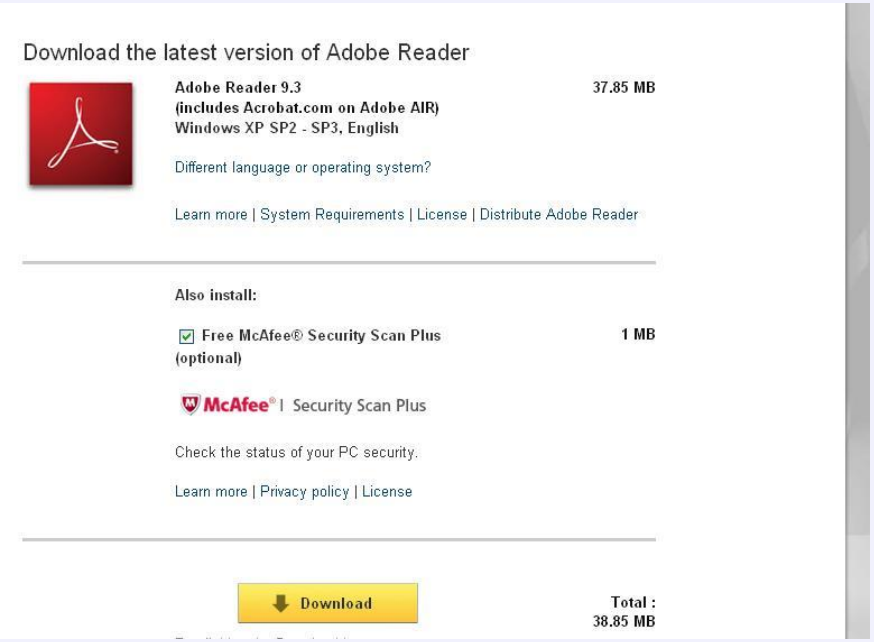
- The numbers are run through public databases to determine whether anyone is using them to obtain credit. If not, they are offered for sale for a few hundred to several thousand dollars.

- 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



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

OWASP
The Open Web Application Security Project

- 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/

HP ships infected keys

OWASP
The Open Web Application Security Project

- 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

OWASP
The Open Web Application Security Project

- 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/

SEC, DOJ, ECPA

OWASP
The Open Web Application Security Project

- for a long time, **the Department of Justice DOJ argued ECPA allowed it to circumvent the Fourth Amendment and access much of your email without a warrant.**.
- **Securities and Exchange Commission SEC, may be doing the same exact thing: it is trying to use ECPA to force service providers to hand over email without a warrant, in direct violation of the Fourth Amendment**.
- ECPA has been used to argue that emails older than 180 days may be accessed without a warrant based on probable cause. Instead, the agencies send a mere subpoena, which means that the agency does not have to involve a judge or show that the emails will provide evidence of a crime.
- https://www.eff.org/deeplinks/2014/04/sec-obtaining-emails-without-warrant-or-not

Utah Cops, Warrantless Search

- Utah law enforcement officials searched, **without a warrant, the prescription drug records of 480 public paramedics, firefighters and other personnel to try to figure out who was stealing morphine from emergency vehicles.**
- **The warrantless search of Utah's database chronicling every controlled substance dispensed by a pharmacist resulted in charges against one paramedic that have nothing to do with the original investigation**. Instead, the authorities discovered an employee whose records exhibited "the appearance of Opioid dependence" and lodged prescription fraud charges against paramedic Ryan Pyle. Now Pyle faces a maximum five-year prison sentence if convicted of the felony.
- http://arstechnica.com/tech-policy/2014/04/utah-cops-warrantlessly-search-drug-records-of-480-emergency-personnel/

Police in North Dakota can now use drones armed with tasers

OWASP
The Open Web Application Security Project

- Police in North Dakota are now authorized to use drones armed with tasers, tear gas, rubber bullets, and other "non-lethal" weapons, following the passage of Bill 1328.
- Sponsored by Rep. Rick Becker (R-Bismarck), the bill was originally intended to limit the police's surveillance powers, and banned all weapons on law enforcement drones. Then a policy lobby group was allowed to amend the bill, though, at which point it only banned lethal weapons, writes *The Daily Beast*.
- http://www.theverge.com/2015/8/26/9211165/north-dakota-armed-drones-tasers

- How soon until these drones get hacked?

Samsung smart fridge leaves Gmail logins open to attack

OWASP
The Open Web Application Security Project

- Pen Test Partners discovered the MiTM (man-in-the-middle) vulnerability that facilitated the exploit during an IoT hacking challenge at the recent DEF CON hacking conference.
- The hack was pulled off against the RF28HMELBSR smart fridge, part of Samsung's line-up of Smart Home appliances which can be controlled via their Smart Home app. While the fridge implements SSL, it fails to validate SSL certificates, thereby enabling man-in-the-middle attacks against most connections.
- The internet-connected device is designed to download Gmail Calendar information to an on-screen display. Security shortcomings mean that hackers who manage to jump on to the same network can potentially steal Google login credentials from their neighbours.
- "The internet-connected fridge is designed to display Gmail Calendar information on its display," explained Ken Munro, a security researcher at Pen Test Partners. "It appears to work the same way that any device running a Gmail calendar does. A logged-in user/owner of the calendar makes updates and those changes are then seen on any device that a user can view the calendar on."
- "While SSL is in place, the fridge fails to validate the certificate. Hence, hackers who manage to access the network that the fridge is on (perhaps through a de-authentication and fake Wi-Fi access point attack) can Man-In-The-Middle the fridge calendar client and steal Google login credentials from their neighbours, for example."
- http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/

Police secretly track cellphones to solve routine crimes

OWASP
The Open Web Application Security Project

- BALTIMORE — The crime itself was ordinary: Someone smashed the back window of a parked car one evening and ran off with a cellphone. What was unusual was how the police hunted the thief.
- Detectives did it by secretly using one of the government's most powerful phone surveillance tools — capable of intercepting data from hundreds of people's cellphones at a time — to track the phone, and with it their suspect, to the doorway of a public housing complex. They used it to search for a car thief, too. And a woman who made a string of harassing phone calls.
- In one case after another, USA TODAY found police in Baltimore and other cities used the phone tracker, commonly known as a stingray, to locate the perpetrators of routine street crimes and frequently concealed that fact from the suspects, their lawyers and even judges. In the process, they quietly transformed a form of surveillance billed as a tool to hunt terrorists and kidnappers into a staple of everyday policing.
- The suitcase-size tracking systems, which can cost as much as $400,000, allow the police to pinpoint a phone's location within a few yards by posing as a cell tower. In the process, they can intercept information from the phones of nearly everyone else who happens to be nearby, including innocent bystanders. They do not intercept the content of any communications.
- http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/

NC Law: Teens who take nude selfie photos face adult sex charges

OWASP
The Open Web Application Security Project

- After a 16-year-old Fayetteville girl made a sexually explicit nude photo of herself for her boyfriend last fall, the Cumberland County Sheriff's Office concluded that she committed two felony sex crimes against herself and arrested her in February.
- The girl was listed on a warrant as both the adult perpetrator and the minor victim of two counts of sexual exploitation of minor - second-degree exploitation for making her photo and third-degree exploitation for having her photo in her possession.
- Psychologist Jeff Temple of the University of Texas Medical Branch said his research has found that **28 percent of teens use their cellphones to send naked photos of themselves to other teens**
- Although the pictures are illegal, **sexual intercourse between 16-year-old teens is not**. The **age of consent for sexual activity in North Carolina is 16**, and **it dips younger than that for teens who are less than four years apart in age**.
- http://www.fayobserver.com/news/local/nc-law-teens-who-take-nude-selfie-photos-face-adult/article_ce750e51-d9ae-54ac-8141-8bc29571697a.html

Foreign Spooks Use Hacked US Data to Root Out Spies

OWASP
The Open Web Application Security Project

- Intelligence services in China, Russia and elsewhere are capitalizing on a treasure trove of recently hacked US government data to identify American spies, according to a new report.
- Foreign powers are using data stolen from the Office of Personnel Management (OPM) in particular and combining it with breached information from healthcare providers like Anthem, infidelity site Ashley Madison, United Airlines, and other firms to build up a digital identity for US intelligence operatives.
- This can then be used to track or even blackmail and recruit US spies, according to the Los Angeles Times.
- US counter-intelligence boss, William Evanina, claimed that this activity can help identify "who is an intelligence officer, who travels where, when, who's got financial difficulties, who's got medical issues, [to] put together a common picture."
- He added that foreign powers were "absolutely" using this information to root out US spies, with unnamed officials pointing the finger at China and Russia as prime culprits.
- http://www.infosecurity-magazine.com/news/foreign-spooks-hacked-us-data-root/

Samsung SmartTV spies on customers

OWASP
The Open Web Application Security Project

- If the walls could talk, they'd probably chat with your Samsung Smart TV: The Internet-connected set may be listening in on users' personal conversations.
- As first reported by The Daily Beast, Samsung's Smart TV privacy policy includes the following warning. "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition," the site says.
- http://www.pcmag.com/article2/0,2817,2476476,00.asp
- Also applies to Motorola Smart Phones, Cars, XBOX360 Kinect, etc

Smart Cars – unsafe at ANY Speed

OWASP
The Open Web Application Security Project

- In July 2015, Chrysler recalled 1.4 million vehicles - researchers were able to control the heating & cooling system, blast the radio, activate the windshield wipers, shut the car down….***from a laptop 10 miles away.***
- GM **OWNSTAR** gadget allows anyone to locate, unlock, or remote start any **GM**, **BMW**, **Mercedes** by intercepting and breaching security of the RemoteLink mobile app.
- **Progressive Insurance** has placed up to **2 million vehicles** at risk of shutdowns, thefts or mysterious accidents by sending drivers the "**Progressive Snapshot"** dongle.

- Perhaps it's time to rename **MADD** as **"Mothers Against Dangerous Developers".**

We Make it Easy (to commit crimes)

OWASP
The Open Web Application Security Project

- 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?

OWASP
The Open Web Application Security Project

Winning The War

Getting it Right

OWASP
The Open Web Application Security Project

- “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

OWASP
The Open Web Application Security Project

- 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

What to teach your Kids, Employees & Interns About Social Media

OWASP
The Open Web Application Security Project

“Everything You Say Can And Will Be Used Against You, By Anybody, Now Or Decades Into The Future.” – Falkvinge

http://www.brainlink.com/free-stuff/webinars/what-to-teach-your-kids-employees-and-interns-about-social-media/

Victory - FBI told 'get a warrant'

OWASP
The Open Web Application Security Project

- The US Department of Justice has moved to quell the ongoing row over the use of IMSI-catchers like Stingray, with a new policy that requires a warrant before they're deployed.
- The policy, announced here, is designed to “establish a higher and more consistent legal standard and increase privacy protections” for the use of cell-site simulators.
- The policy takes effect immediately and applies across all DoJ agencies.
- The policy also addresses the understandable fear that anyone's cellphone use could be caught by the devices, merely because they happened to be in the same place at the same time as a Stingray was in use.
- The DoJ statement notes that the policy “includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, when the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.”
- The controversial devices have been under attack from the ACLU, and lawyers in the US are working through FBI use of Stingrays in case convictions can be appealed.
- The new policy has been welcomed by House Oversight and Government Reform Committee Chairman Jason Chaffetz, who released this statement on TwitLonger.
- “As I’ve long stated, establishing a high uniform standard helps protect personal privacy and discourages abuse and mishandling of these powerful devices,” he wrote.
- He states that the battle isn't over, since there's still secrecy around the use of geolocation technology, and Chaffetz says the DoJ should ”continue to produce information – including the Jones memos – to help Congress and the public understand how the federal government tracks people.”
- http://www.theregister.co.uk/2015/09/04/stingray_stung_fbi_told_get_a_warrant/

Victory - Baltimore lawyers vow to review 2,000 FBI Stingray snoop cases

OWASP
The Open Web Application Security Project

- Defense attorneys in Baltimore, US, are planning to reexamine 2,000 police arrests made with the assistance of Stingray – the cellphone surveillance equipment that identifies and logs mobile device owners within range.
- A group of lawyers including the city's public defender want to get a closer look at whether they can challenge some of the arrests made in part on evidence gathered by the secretive phone-tracking tool.
- The legal eagles believe the cops' use of the technology was excessive and unconstitutional in some or all cases – and wants any convictions thrown out if necessary.
- "This is a crisis, and to me it needs to be addressed very quickly," Baltimore public defender Natalie Finegar told USA Today, though Finegar conceded to the Baltimore Sun that "it's going to be a labor-intensive process.“
- http://www.theregister.co.uk/2015/08/28/baltimore_stingray_cases/

Victory - FTC COMMISSIONER SUPPORTS ENCRYPTION

OWASP
The Open Web Application Security Project

- High profile car hacks, large-scale breaches of intimate information, news of compromised household appliances -- hardly a day passes without some revelation of the ways in which our increasing interconnectedness is introducing new vulnerabilities into our lives. Technology is advancing at a rapid clip, and so are breaches. Now, more than ever, strong security and end-user controls are critical to protect personal information.
- Each of us can play an important role in protecting our information on laptops, desktops, and smartphones by using strong end-user controls, such as disk encryption and firmware passwords. Disk encryption can protect information stored on the hard-disk from unwanted access and hardware passwords essentially prevent machines from being used without the password.
- Using these tools can also make it easier for consumers to recover lost or stolen devices as the FTC's Chief Technologist recently discovered through personal experience.
- Encryption and end-user protections can raise issues of access for law enforcement. Some argue that data storage and communications systems should be designed with exceptional access -- or "back doors" -- for law enforcement in order to avoid harming legitimate investigative capabilities. However, many technologists contend that exceptional access systems are likely to introduce security flaws and vulnerabilities, weakening the security of products.
- This debate, sometimes called the crypto wars, is hardly new -- it has been going on in some form or another for decades. But what is changing is the extent to which we are using connected technology in every facet of our daily lives. **If consumers cannot trust the security of their devices, we could end up stymieing innovation and introducing needless risk into our personal security. In this environment, policy makers should carefully weigh the potential impact of any proposals that may weaken privacy and security protections for consumers.**
- http://m.huffpost.com/us/entry/8083756 **Terrell McSweeny Commissioner, Federal Trade Commission**

Victory – FTC vs Wyndham: **Cybersecurity Under FTC Authority**

OWASP
The Open Web Application Security Project

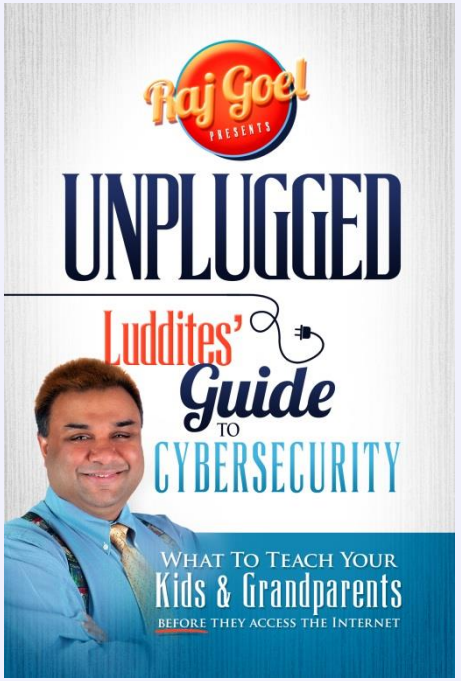
- U.S. appellate court granted the Federal Trade Commission (FTC) authority to regulate corporate cybersecurity.
- Under its new powers, the FTC will continue to "prevent business practices that are anticompetitive, deceptive or unfair to consumers; enhance informed consumer choice and public understanding of the competitive process; and accomplish this without unduly burdening legitimate business activity." But, the agency now has been given the mantle to protect online security.
- 2015 FTC won vs Wyndham
- 2015 – FTC is suing Anthem
- 2012 - **FTC fines RockYou $250,000 for storing user data in plain text**
- 2012 **- FTC tears into Apple, Google over kids' privacy – or lack of**
- 2011 **– FTV vs RITEAID**

- Read the **LESSONS LEARNED FROM THE FTC** presentation at http://www.rajgoel.com/presentations/

Discuss With Your Kids & Grandparents

OWASP
The Open Web Application Security Project

Protect Your Home & Family
Chapter 1 - Parenting Responsibly In The Internet Era
Chapter 2 - Has Social Media Gone Unsupervised For Far Too Long?
Chapter 3 - Grandparents Are Offering Their Grandkids To Predators
Chapter 4 - Prevent Your Kids From Spending Thousands On In-App Purchases
Chapter 5 - The Fine Line Between Guidance And Surveillance
Right To Privacy In The 21st Century
Chapter 6 - The Right To Digital Privacy
Chapter 7 - The Paradox Of Not Owning What You Buy
Chapter 8 - The Myth Of Online Privacy
Chapter 9 - Information To The Highest Bidder: The Data Exchange Between Government And Private Business
Chapter 10 - Invasion Of Privacy: Is It The User's Fault?
Chapter 11 - Ad Blockers Make The Web Safer And Faster!
The Banes Of Technology
Chapter 12 - Lessons Learned From Centcom, Crayola And Isis Hackers
Chapter 13 - The Real Cost Of Facebook
Chapter 14 - How You Spend Your Time Online Can Be Used Against You
Chapter 15 - Adult Friend Finder Data Breach – Blackmail R Us?
Chapter 16 - Welcome To The Age Of Online Dating
Chapter 17 - Social Security Is Not Secure
Chapter 18 - Beware The Smart Home Of The Future
Smart Cars: Unsafe at Any Speed

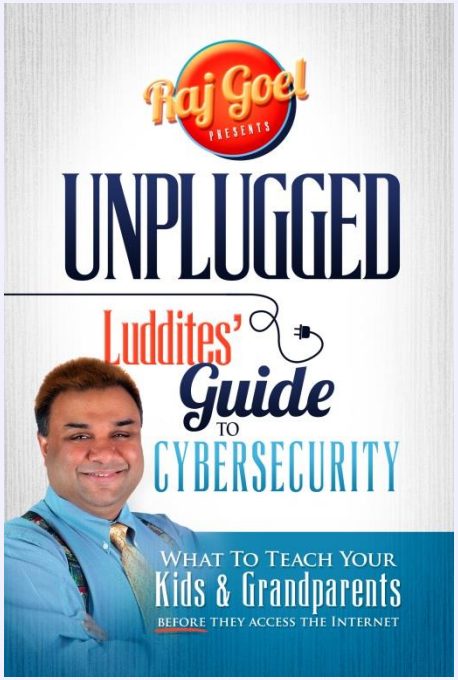


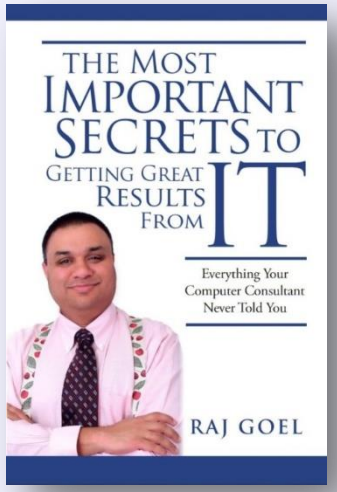
Contact Information

OWASP
The Open Web Application Security Project

Raj Goel, CISSP

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





Author of

UNPLUGGED Luddites Guide To Cybersecurity
http://www.amazon.com/UNPLUGGED-Luddites-Guide-CyberSecurity-Grandparents/dp/0984424830/

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