ELECTRONIC CRIMES INC: THE MOST PERVASIVE CRIME PROBLEM OF THIS MILLENNIUM

Chris Swecker
Attorney at Law
chris.swecker@sweckerlaw.com

THE CYBER ENVIRONMENT
"IT'S A BAD NEW WORLD"

Sony CEO

SCOPE OF FRAUD LOSSES: OVER $620 BILLION INDUSTRY

Fraud Type	Annual Losses in Billions
Health Care Fraud (NHCAFA and CBO)	80 Billion
Insurance Fraud (NICB)	40 Billion
Mortgage Fraud (FBI/MBA)	40 Billion
Identity Theft (Javelin)	21 Billion
Stimulus Grant Fraud (RAT Board)	40 Billion
Payments Fraud (Lexis Nexus)	200 Billion
Trade Fraud (Zdanowiczj)	200 Billion

3

THE PERFECT CYBER STORM

- Hacktivists- Capable and Issue Driven;
- Criminals- Professional Criminals Operate in Virtual Criminal Networks. May Be for Hire;
- Cyber Terrorism
- Government Hackers- Most Skilled, Unlimited Resources, Creative and Highly Motivated.
- Cyber Extortionists (Cryptolocker)

WHO ARE THOSE GUYS?

5

STEP ASIDE US MAFIA, THE RUSSIANS ARE COMING: A NEW CRIME PARADIGM

6

OUTDATED ORGANIZED CRIME BRICKS AND MORTAR MODEL

- Extortion
- Drugs
- Bribery
- Gambling
- Loan Shark Operations
- Cargo Theft
- Labor Racketeering
- Protection Payments
- Pump and Dump
- Hijacking
- Bid Rigging/Contract Fraud

7

DRUG CARTELS - PROFITABLE ENTERPRISE BUT VIOLENT AND RISKY

U.S. government estimates suggest that Mexican and Colombian drug trafficking organizations earn between $18 billion and $39 billion annually from sales in the United States.

The life of a drug kingpin is “nasty, brutish an

8

CATALYST FOR A NEW CRIME PARADIGM: NOVEMBER 1989

Russian Mob, and KGB Run The Black Market

The "Krysha Model" Integrates Criminal and Legal Economies

The Wall Comes Down

9

EURASIAN CRIME IN THE USA

Strongholds

- Brighton Beach, NY
- Glendale, CA
- Miami, Fla.
- Chicago, Ill
- San Francisco CA
- Philadelphia, PA.
- Newark, NJ

Focus

- Health Care Fraud
- Insurance Fraud
- Internet Fraud
- Credit Card Fraud
- ATM Skimming
- Internet Fraud Schemes
- Corporate Account Takeover

10

FINANCIAL CRIMES "CRIMINOGENIC" ENVIRONMENT

- Financial Crimes Networks Increase In Number and Sophistication and Continually Innovate to Cause Huge Dollar Losses and Risk to Reputation/Brand
- The Bad Guys Enjoy a Significant Advantage By Exploiting Persistent Silos Across all Industries and Government Benefit Programs
- Good Guys Are Being Out-networked
- To Slow and Reverse Down the Massive Losses We Must Change Our Strategies

11

TOP SIX BENEFIT PROGRAMS

- SSI
- SNAP
- WIC
- Unemployment Insurance
- MEDICAID
- Medicare

- In 2009, 19.0 percent of U.S. families, on average, participated in at least one major means-tested program per month.

12

HEALTH CARE FRAUD: OVER $1.1 BILLION IN FOUR CASES

LAW ENFORCEMENT TOO FAR FROM THE ACTION

$163 Million

October 2010
73 Indicted

$200 million

February 2011
91 indicted

$295 million

September 2011
20 Indicted

$430 million

October 2012
91 Indicted

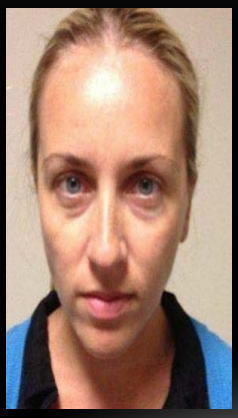
13

ARMEN KAZARIAN: TOP THIEF IN LAW

- Top level "Vor," or "Thief-in-Law" referring to a select group of high-level criminals from Russia and the countries that had been part of the former Soviet Union, including Armenia
- In July 2011 sentenced in Manhattan federal court to 37 months in prison for his involvement with the Mirzoyan-Terdjanian Organization
- Set up 118 imaginary health clinics to rack up more than $100 million in billings for patients and procedures that never existed
- Used postal addresses in 25 states, using the stolen identities of real doctors. Then they used stolen patient data from Orange Regional Medical Center in Middletown

14

MEDICAID MILLIONAIRES

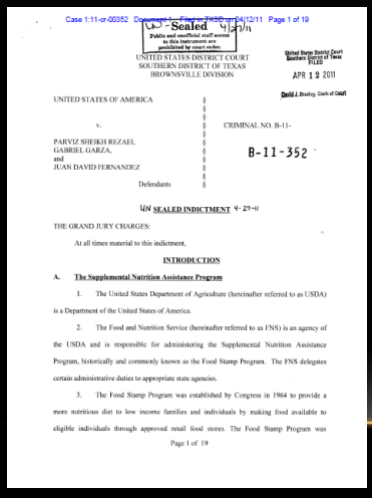


- Oceana complex in Brighton Beach boasts seaside condos, marble lobbies, indoor and outdoor swimming pools — and six residents busted for Medicaid fraud.
- Kristina Zelinsky, 34, became the sixth resident since 2011 charged with Medicaid fraud in what prosecutors say is a growing trend. Zelinsky was indicted for allegedly scamming more than $25,000 from the taxpayer-funded health care system designed to help the needy. Prosecutors say that during the decade she claimed to be destitute, she got an $850,000 mortgage for an Oceana condo, owned three cars

  Read more:
  http://www.myfoxny.com/story/23199865/resident-of-luxury-brooklyn-condo-indicted-for-medicaid-fraud#ixzz2jWoGDTrz

15

"YOU GOTTA PLAY THE GAME, PLAY THE SYSTEM"



Case 1:11-cr-00352 Document 1 Filed in TXSD on 04/12/11 Page 1 of 19

Sealed

Public and unofficial staff access to this instrument are prohibited by court order.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
BROWNSVILLE DIVISION

United States District Court
Southern District of Texas
FILED
APR 12 2011
David J. Bradley, Clerk of Court

UNITED STATES OF AMERICA
v.
PARVIZ SHEIKH REZAEI,
GABRIEL GARZA,
and
JUAN DAVID FERNANDEZ
Defendants

CRIMINAL NO. B-11-

B-11-352

UNSEALED INDICTMENT 4-27-11

THE GRAND JURY CHARGES:

At all times material to this indictment,

INTRODUCTION

A. The Supplemental Nutrition Assistance Program

1. The United States Department of Agriculture (hereinafter referred to as USDA) is a Department of the United States of America.

2. The Food and Nutrition Service (hereinafter referred to as FNS) is an agency of the USDA and is responsible for administering the Supplemental Nutrition Assistance Program, historically and commonly known as the Food Stamp Program. The FNS delegates certain administrative duties to appropriate state agencies.

3. The Food Stamp Program was established by Congress in 1964 to provide a more nutritious diet to low income families and individuals by making food available to eligible individuals through approved retail food stores. The Food Stamp Program was

Page 1 of 19

- 3.8 million dollar loss
- Multiple defendants and storefronts
- 4 Year Long Scheme
- Food stamp fraud
- Wire fraud
- Money laundering
- Money structuring
- Unlicensed money transaction business

16

THE FOOD-STAMP CRIME WAVE

THE NUMBER OF FOOD-STAMP RECIPIENTS HAS SOARED TO 44 MILLION FROM 26 MILLION IN 2007.

- The USDA's Food and Nutrition Service now has only 40 inspectors to oversee almost 200,000 merchants that accept food stamps nationwide.
- Wisconsin: nearly 2,000 recipients claimed they lost their card six or more times in 2010 and requested replacements."
- Wichita, Kansas : 13 people indicted in food stamp fraud case March 2011 ($360,000)
- Phoenix, Arizona: 18 Indicted in Food Stamp Fraud Investigation July 2011 ($700,000
- $8 million food stamp fraud mastermind pleads guilty to scam in New York City (City Human Resources Administration).

17

DATA COMPROMISE

The Most Pervasive Crime Problem of this Millenium

"CYBERCRIMINALS DON'T STRIKE IN ONE PLACE AND THEY DON'T WORK ALONE." DEE RADCLIFFE EC MAG

- Gonzalez and his accomplices
  - Communicated over carder forums
  - Their network spanned from San Diego to Estonia
  - Hacked into wireless point-of-sale (POS) and store networks by war-driving from parking lots. In the case involving Heartland, the suspects used SQL injection attacks
  - Two Russian co-conspirators hacked into corporate computer networks and secretly placed "malware," or malicious software, that allowed them backdoor access to the networks later to steal data
  - Indicted by U.S. DOJ with stealing more than 130M account numbers from card processor Heartland Payment Systems, 7-Eleven, others

GLOBAL BUSINESS ENVIRONMENT

- IP is Core Business Asset;
- PII stored in IT system or utilized for payments;
- Few CISO Positions, IT Securty is an Ancillary Duty;
- Open Work Environment;
- Global Footprint With Multiple Sites in High Risk Areas;
- Corporate Executives Not Sufficiently Aware of Full Scope of Threats
- Reliance on Internet
- All Data and Data Bases Treated the Same

HOMELAND SECURITY CYBER PROJECT: GENERAL THREAT FINDINGS

- General Findings
  - Owners who outsource assume security is rolled into the service they are buying (it is not)
  - Largely, very little to no formal security policies or IT policies exist
  - No application of "defense in depth"
  - Lack of security trained personnel on-site
  - No active patch management performed
- Network Scan Results
  - All companies had some sort of nefarious activities, even ones with industrial grade enterprise security suites
  - **Most common threat appears to originate from Russian Business Network actors**
  - No APT detected over 4 week-long scans (Scanned 7 of 9 participants)
  - Most/all vulnerabilities could have been avoided through common security practices

SPECIFIC THREATS FOUND

Specifically, CTB analysts discovered the following vulnerabilities:

- About 20 percent of one CTB participant's network computers were observed communicating with questionable IPs within the "co.kr", "com.cn", "com.ru", and "co.cc" domains.
- Numerous servers across all participants appeared to be compromised with:
  - Domain Name Server (DNS) exploits
  - Directly connecting to known Russian Business Network (RBN) IP addresses
  - Connecting to questionable domains such as www.h-r-connect.co.cc, as well as other co.cc domains.
  - Observed backdoors, Trojans and rootkits on two Unix based servers
- DropBox, a cloud storage service which has many associated vulnerabilities, was being used extensively to store company related data for two of the nine CTB participants
- The number of patches missing ranged between 112 and 742
- As high as 40% of computers at one site were observed communicating with known RBN IPs
- BotNet related activity was noted on one-third of the computers one particular network\

MASS COMPROMISES

The Early Compromises

- TJMax/Heartland/Hannaford: over 200 million PII
- RSA : Spear-phishing attack: undisclosed number
- Epsilon: 2500 corporate customers, millions of email addresses
- Sony: over 77 million user accounts and Credit Card data
- RBS Worldpay: $9 million loss, 1.5 million PII
- Texas Comptroller's Office
- USAirways: PII of 3,000 pilots
- Michaels: POS skimmers

Recent Compromises

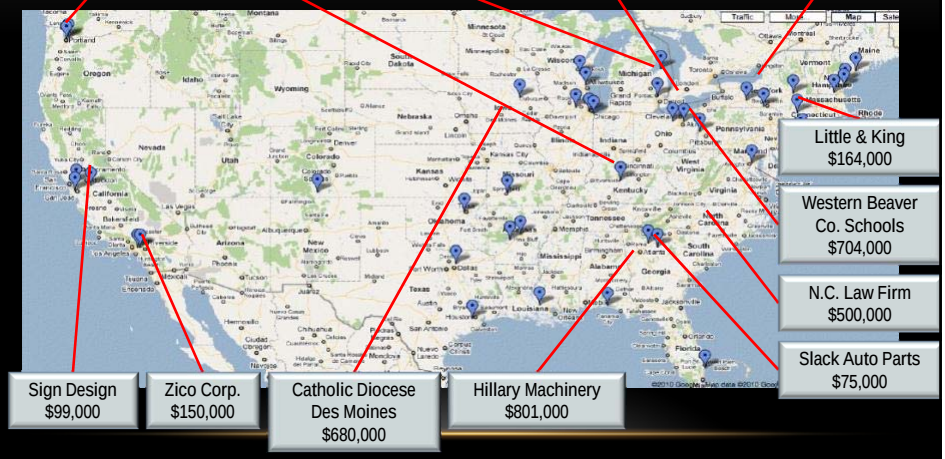
- Target
- Home Depot
- Chase
- Stratfor

RUSSIAN BUSINESS NETWORK

Per annual Verizon/U.S. Secret Service 2012 report
83% of compromised computer records were attributed to organized crime.
67% emanated from eastern Europe.

24

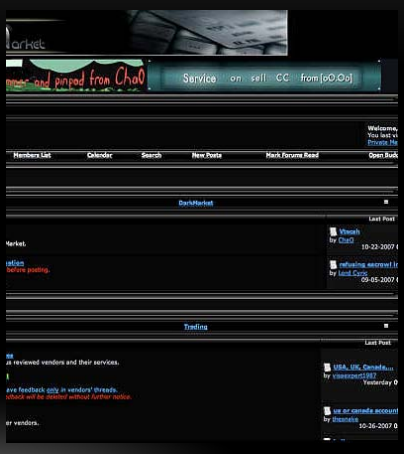
ACCOUNT TAKEOVER IMPACTS BUSINESSES AND PRESENT LEGAL CHALLENGES



- Source: www.krebsonsecurity.com, all dots total $40MM gross losses

2102 RAND STUDY OF DARK MARKETS

- The hacker market has in some respects become more profitable than the illegal drug trade. The data hackers steal ends up on a network of illegal trading sites where they buy and sell large amounts of personal data for profit.



MONEY MULES:

Indicators

- Student or temporary work Visas
- April to late September
- Mules open multiple bank accounts
- Mules share addresses
- Common accounts
- Frequent International money wires
- Personal accounts with high velocity transfers business account
- Eastern European Passports

Function Like "Smurfs"

27

OPERATION TRIDENT BREACH: THE CRITICAL ROLE OF "MONEY MULES"

28

OREGON DATA BREACH

- Names, birth dates, Social Security numbers, and other personally identifiable information belonging to about 850,000 job seekers in Oregon was exposed after hackers gained illegal access to a database containing the information at the State Employment Department. The names were part of the WorkSource Oregon Management Information System and pertained to individuals looking for jobs at state employment offices.

UTAH DEPARTMENT OF HEALTH

- The health information and PII of more than 780,000 Utah citizens were put at risk when Eastern European hackers broke into a server maintained by the Utah Department of Technology Services this spring by taking advantage of poor authentication configuration following database migration to a new server.
- *Lessons Learned:* Poor authentication controls, uneven patch management, and dicey configuration management add a inordinate amount of risk to the database protection equation.

NEW HAMPSHIRE DEPARTMENT OF CORRECTIONS

- In a case of the foxes running the hen house, the New Hampshire Department of Corrections found that inmates at a state correctional facility were able to access the main offender management database system. How so? That system was linked to a server that inmates working in the prison industries shops used. Access to the system would allow inmates to change items like parole dates and sentencing information, as well as view personally identifiable information on prison staff members.
- *Lessons Learned:* This case offers a stark example of why uber sensitive databases require special segmentation measures to keep them safe from side-channel attacks.

THE SOUTH CAROLINA DEPARTMENT OF REVENUE INTRUSION

Successfully Targeting the Crown Jewels of Personal Data

S.C. Exposure on Account Takeover

2011 FBI Stats	Account Takeover
400	Investigations
$85,000,000	Actual Losses
$212,000	Average Loss

2012 S.C.	Business Tax Return Breach
676,000	Stolen Records
1,000	Potential A.T. Victims
$212,000,000	Potential Losses
$30,000,000	Potential Litigation Expense

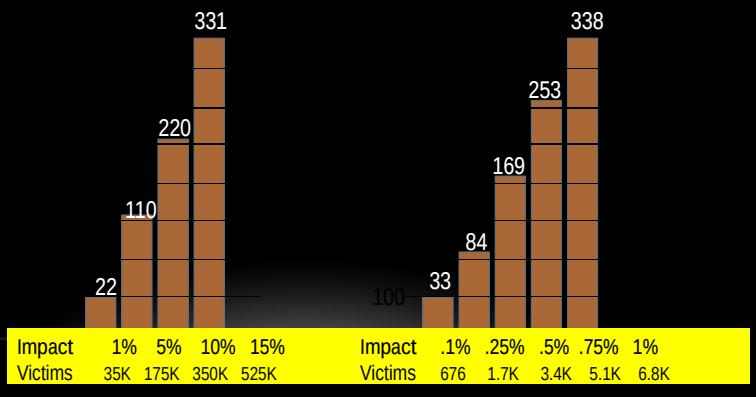
http://www.infosecisland.com/blogview/16536-FBI-Investigating-Over-400-Corporate-Account-Takeovers.html

3333

S.C. DOR Hack

Individual ID Theft
3.5MM Records
Avg. Clean Up = $631*

Bank Account Takeover
676,000 Records
Avg. Loss = $50,000**



34

* 2011 Javelin ID Fraud Survey, ** Use 25% of ACFE and FBI Average Reported Acct Takeover Fraud Loss of $200K

CORPORATE ESPIONAGE

Outdated Espionage Model

Espionage 2012

THREAT COUNTRIES – STATE-SPONSORED CYBER ESPIONAGE

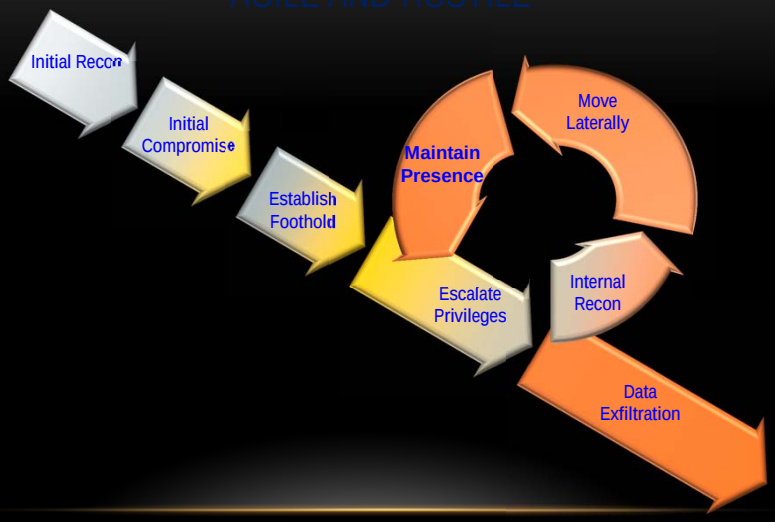
- China
- Russia
- Iran
- North Korea
- Israel
- India
- Pakistan

FBI WARNS OF CYBERATTACKS LINKED TO CHINA
THE FBI AND SECURITY COMPANIES HAVE OBSERVED 'RECENT INTRUSIONS'

BY JEREMY KIRK (TECHWORLD) PUBLISHED: 16 OCTOBER 2014

- "The FBI has recently observed online intrusions that we attribute to Chinese government affiliated actors," according to the FBI statement. "Private sector security firms have also identified similar intrusions and have released defensive information related to those intrusions."
- The U.S. government had continued to be vocal about cyberattacks and has directly called on China for greater cooperation. China has maintained it does not coordinate cyberattacks against U.S. companies and organizations and maintained it is a victim of such attacks as well.
- Security companies Cisco, FireEye, F-Secure, iSIGHT Partners, Microsoft, Tenable, ThreatConnect, ThreatTrack Security, Volexity, Novetta and Symantec said they conducted their first joint effort aimed at stopping hackers affiliated with "Operation Aurora," which struck 20 companies in 2009, including Google.

ANATOMY OF AN INTRUSION: AGILE AND HOSTILE



APT: WHAT ARE THEY AFTER?

OBJECTIVE	INFORMATION	EXAMPLES
Intelligence	Research & Development	China Sea Exploration Results
	Corporate Strategy	Senior Exec E-Mail
	Litigation Strategy	Law Firm Case Material
	Government Direction	Monetary policy
	Weapons Systems	F35 Lightning Fighter Jet
	Negotiation Positions	Merger/Acquisition Plans

WHAT SETS APT APART?

- They have thousands of custom versions of malicious code (malware) that circumvent common safeguards such as anti-virus
- They escalate the sophistication of their tools and techniques as a victim's capability to respond improves
- They maintain their presence within the victim network and, if lost, they repeatedly seek to regain that presence
- They target vulnerable people more often than they target vulnerable systems
- They specifically target victim firms — the intrusions are very different from commodity threats and other targeted attacks by organized crime syndicates

FACTS

- Of 44 Fortune 500 companies subjected to Threat Assessment Process (TAP) 43 Were Determined to Have Malicious Chinese Malware On Their System and Sensitive Data Exfiltrated;
- All Started With Email PDF, PPT, Excel or Word Attachments;
- CEO Specifically Targeted;
- Intruders Commonly target email for marketing and pricing materials;
- Will Also Target Accounting and Law Firms Especially During Merger and Acquisition Activity;
- SEC filings and Public records show Dow and DuPont were hit hard by Chinese;

41

STATE SPONSORED ECONOMIC ESPIONAGE

The three main Chinese government units that run intelligence operations are:

- The Ministry of State Security,
- The Military Intelligence Department of the People's Liberation Army and
- A small group known as the Liaison Office of the General Political Department of the Chinese army.

CHINESE AGRICULTURAL RESEARCHER CHARGED UNDER ECONOMIC ESPIONAGE ACT FOR TRADE SECRET THEFTS AT DOW AND CARGILLL

- On July 13, 2010, Kexue a/k/a "John" Huang, 48, a Chinese national who had been granted legal permanent resident status in the United States and a former resident of Carmel, Ind., was arrested in Westborough, MA and indicted on 17-counts in the Southern District of Indiana for misappropriating and transporting trade secrets to the People's Republic of China (PRC) while working as a research scientist at Dow AgroSciences LLC
- From January 2003 until February 2008, Huang was employed as a research scientist at Dow, where in 2005 he became a research leader in strain development related to unique, proprietary organic insecticides marketed worldwide.
- Huang admitted that while employed at Cargill, he stole a key component in the manufacture of a new food product, which he later disseminated to a student at Hunan Normal University in the PRC.
- The aggregate loss from Huang's criminal conduct allegedly exceeded $7 million but was less than $20 million

EXAMPLES

Recent Insider Thefts of Corporate Trade Secrets With a Link to China

David Yen Lee…chemist with Valspar Corporation…between late 2008 and early 2009 used access t internal computer network to download about 160 secret formulas for paints and coatings to his ow storage media…intended to take this proprietary information to a new job with Nippon Paint in Shanghai, China…arrested March 2009…pleaded guilty to one count of theft of trade secrets; sentenced in December 2010 to 15 months in prison.

Meng Hong…DuPont Corporation research chemist...in mid-2009 downloaded proprietary information on organic light-emitting diodes (OLED) to personal e-mail account and thumb drive…intended to transfer this information to Peking University, where he had accepted a faculty position; sought Chinese Government funding to commercialize OLED research…arrested October 2009…pleaded guilty to one count of theft of trade secrets; sentenced in October 2010 to 14 months in prison.

Yu Xiang Dong (aka Mike Yu)…product engineer wjth Ford Motor Company who in December 2006 accepted a job at Ford's China branch…copied approximately 4,000 Ford documents onto an external hard drive to help obtain a job with a Chinese automotive company…arrested in October 2009…pleaded guilty to two counts of theft of trade secrets; sentenced in April 2011 to 70 months in prison.

PROGRAM “863”

- “In stealing, transferring and using the trade secrets, Kexue Huang, a/k/a ‘John,’ intended to benefit Hunan Normal University, the national Natural Science Foundation and the 863 Program. Each of these entities is a foreign instrumentality of the People’s Republic of China,” the Huang plea agreement said.
- Program 863 is known as the “National High Technology Research and Development Program of China,” according to the indictment.

45

CHINESE THREAT: SPEARPHISHING

- Chinese intelligence and military units, and affiliated private hacker groups, actively engage in "target development" for spear-phish attacks by combing the Internet for details about commercial employees' job descriptions, networks of associates, and even the way they sign their emails,
- Spear-phish attacks are "the dominant attack vector.
- Remote Access Trojans (RAT) are often used with Poison Ivy Variation.

46

MORE CHINA FACTS

- An estimated 1.6 billion attacks are launched from China each month, with some successful efforts breaching the computer systems of the Pentagon and those of the French, German and British governments.
- In 2009, investigators discovered that Ghostnet, the largest-ever network of cyber attacks, could be traced back to China. The operation's command and control gained real-time control over 1,200 computers belonging to foreign embassies, international organizations and media groups in more than 100 countries according to experts,
- The biggest threat posed by attacks traced to China is the loss of industrial secrets.

MITIGATIONS

Compromise And Fraud Is Not Inevitable

"COMPUTER MATCHING"

- The Computer Matching and Privacy Protection Act of 1988 (Pub. L. 100-503), as amended, revised the Privacy Act to add procedural requirements that agencies must follow when matching certain electronic databases.
- The requirements include formal matching agreements between agencies, notice in the Federal Register of the agreement before matching may occur, and review of the agreements by Data Integrity Boards at both agencies.
- The Act provides an exemption for law enforcement from these administrative requirements, the exemption applies only when a specific target of an investigation has been identified.
- In 2010, the *Patient Protection and Affordable Care Act* amended the CMPPA to exempt matches performed by the U.S. Department of Health and Human Services or its Inspector General related to potential fraud, waste, or abuse.
- Inspector Generals are seeking an IG exemption.
- GAO exempt so it is free to conduct studies and expose missed matching opportunities.

49

SSA MATCHING PROJECTS

- SSA saved $580 million per year from OASDI prisoner suspensions by matching prisoner data from corrections facilities monthly against the Agency's OASDI and Supplemental Security Income (SSI) records, halting benefit payments to prisoners.
- For FY 2011, the Agency expects to save $100 million, and by 2013, SSA projects approximately $900 million in lifetime program savings for each year the Agency uses Automated Access to Financial Information (AFI) to match unreported assets or absence from the US for over 30 days.
- *Individuals Receiving Benefits Under More than One Social Security Number at Different Addresses*
- *SSI Recipients with Unreported Real Property*
- *OASDI Benefits Affected by State or Local Government Pension*
- *SSI Recipients Who Alleged Being Separated or Divorced*
- *Follow-up: Survivors' Benefits Paid in Instances When SSA Removed the Death Entry from a Primary Wage Earner's Record*

50

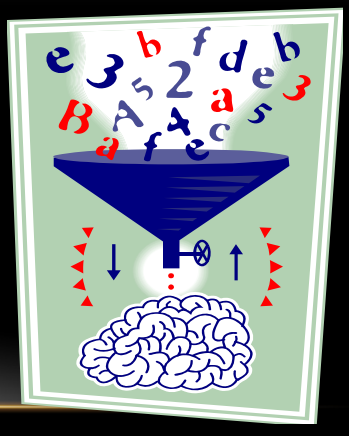
CASE IN POINT

- [Federal Register Volume 76, Number 156 (Friday, August 12, 2011)] [Notices] [Pages 50198-50199] From the Federal Register Online via the Government Printing Office [www.gpo.gov] [FR Doc No: 2011-20608]
- DEPARTMENT OF EDUCATION Privacy Act of 1974; Computer Matching Program AGENCY: Office of the Inspector General, U.S. Department of Education. ACTION: Notice of computer matching between the U.S. Department of Education and the U.S. Office of Personnel Management
- This program will assist in verifying the income information reported by Federal employees on the FAFSA. ED will compare the FAFSA income to the income listed in OPM/GOVT-1 General Personnel Records System (71 FR 35342, June 29, 2006).

51

THE ROLE OF ANALYTICS: FRAUD RINGS LEAVE A TRAIL OF DATA THAT TRANSCENDS SILOS

- Email address
- PO Box
- IP address
- Phone number
- Physical address
- Account Number
- Personally Identifiable Information
- Electronic device profile



52

STEPS TOWARDS MORE EFFECTIVE ENTERPRISE RISK MANAGEMENT

- Assessment of current state
  - Architecture
  - Risk Components
  - Data
  - Corporate Culture
  - Process
- Identify and prioritize risks
- Data Security/Segmentation
- Active Monitoring
- Network Scan
- Briefing and Feedback

PHASE 2-ENTERPRISE RISK MANAGEMENT

- Design Enterprise Risk Governance Structure
  - End to End Consolidated Security Strategy
  - Converge Physical and IT Security
  - Training and Awareness
  - Corporate Culture
  - Metrics and Dashboards
  - Incident Management
  - Business Continuity
  - Screening and Monitoring
  - Supply Chain Security

PERSONAL SECURITY

- Patch Updates
- Extra Authentication
- Keep a close eye on credit card and banking activity
- Take extreme care with online banking access: scramble userid and password keystrokes
- Shred
- Protect Data
- Educate yourself about phishing
- Lock down credit info

QUESTIONS?