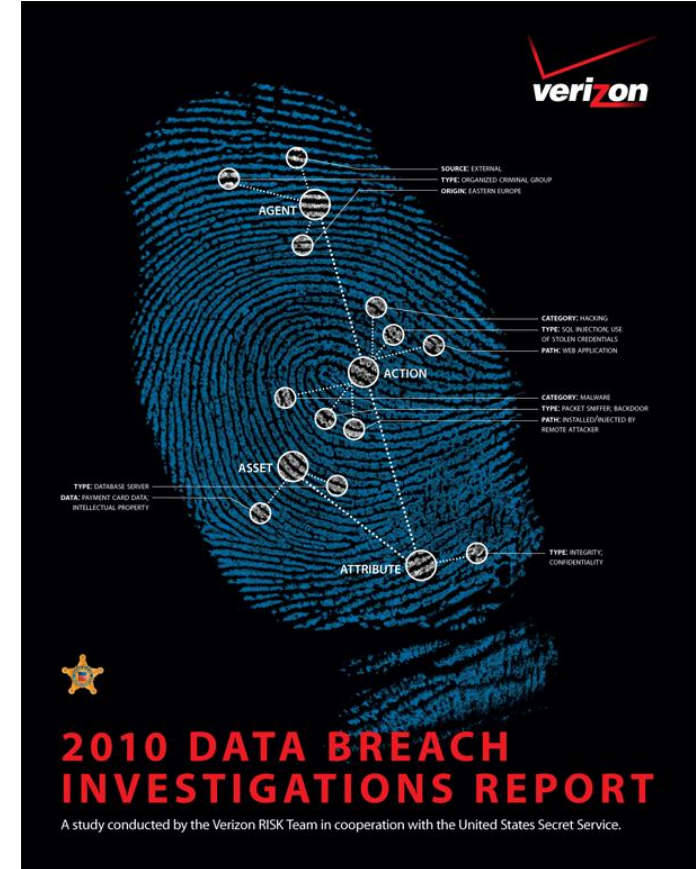


2010 Data Breach Investigations Report



Paul Wright, MSc EnCE, CFIA, CHFI, CSTA, QSA
MEA Principal Consultant, Investigative Response



Remember

- **Partnerships**
- **e-Crime Prevention**
- **Education, Education, Education**
- **e-Voids**
- **Digital Intelligence**

“Catch me if you Can!”



Methodology

Data Source

- Verizon Business Investigative Response Team
- **NEW:** United States Secret Service (USSS)

Collection and Analysis

- VERIS framework used to collect data after investigation
 - USSS used internal application based on VERIS
- Case data anonymized and aggregated
- RISK Intelligence team provides analytics

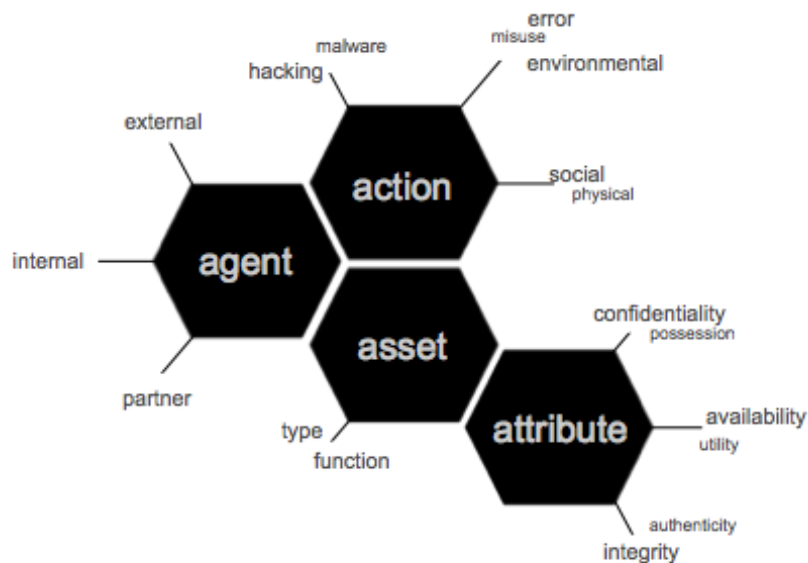
Data Sample

- Six years of forensic investigations (not internal Verizon incidents)
- >900 breaches, 900 million stolen records in combined dataset
 - Actual compromise rather than data-at-risk
 - Both disclosed and non-disclosed
 - Many of the largest breaches ever reported

VERIS Framework

VERIS is a set of metrics designed to provide a **common language for describing security incidents** (or threats) in a structured and repeatable manner.

The Incident Classification section employs Verizon's **A⁴ threat model**



A security incident (or threat scenario) is modeled as a series of **events**. Every event is comprised of the following 4 **A**'s:

Agent: Whose actions affected the asset

Action: What actions affected the asset

Asset: Which assets were affected

Attribute: How the asset was affected

2010 Data Breach Investigations Report

e-Crime Prevention

e-Crime Prevention

- Keyloggers
 - Skimmers
 - Law Firm (example)
- Passwords
 - Policy Review and Default after a restore
 - Remote Access via home computers
 - Third party use of passwords
- Education, Education, Education
 - War Games (example)
- USB's and other external computer storage media
- Social Engineering
 - Facebook and LinkedIn
 - Presentation at a Financial Institution (example)

e-Crime Prevention

- Intelligence 'harvest' of the Internet
 - Confidential Information
- Do your Processes align to your Policies
 - Shredders and Patching
 - Password policy and a Point of Sale application
- Unknown Unknowns
 - Do you know where your data is?
 - Scoping an Investigation
 - Do you know who has access to your system?
 - Do you know your network and what systems you have?
- Outsourcing
 - Low hanging fruit
- E-Crime prevention will reduce the likelihood of a hi-tech or e-crime taking place

First Responder and Triage

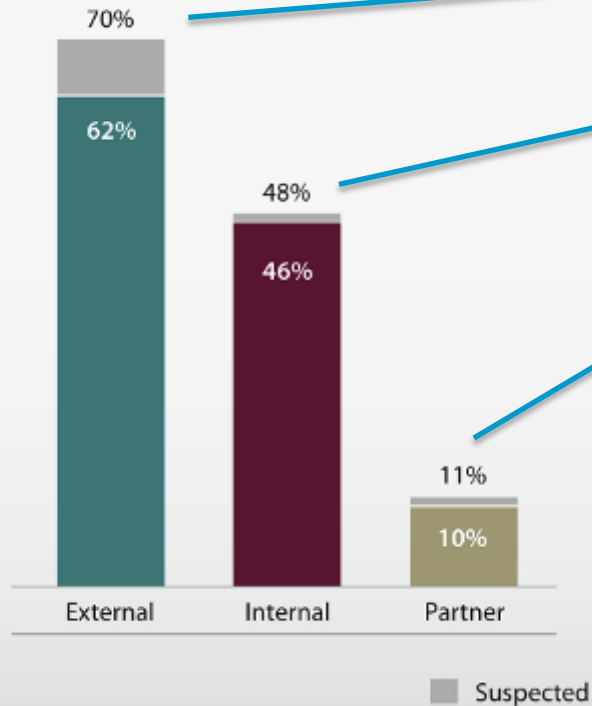
- Polices, Procedures, Guidelines and Best Practices
 - Must align with First Responder and Triage PPP's
 - Are they local, regional, national or global
- Encryption
 - Forwarded, Duplicated, Stored elsewhere
- Crisis Management
 - Do you practice?
- We find that the initial information is different to what actually took place
 - Solution, business incident response plans
- Most information is usually available to an organisation if they know where and how look
- Who should be a 'First Responder'
 - Training

2010 Data Breach Investigations Report

RESULTS & ANALYSIS

Threat Agents

Figure 5. Threat agents (inclusive) by percent of breaches



70 %
48 %
+ 11 %
COLLUSION

Figure 8. Compromised records by threat agent, 2009

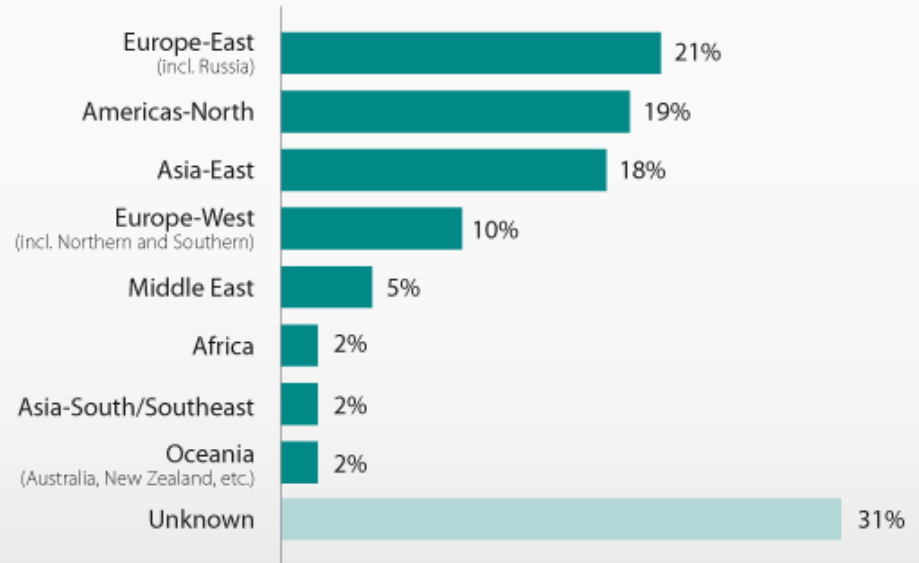


External Agents

Table 1. Types of external agents by percent of breaches within External

Organized criminal group	24%
Unaffiliated person(s)	21%
External system(s) or site	3%
Activist group	2%
Former employee (no longer had access)	2%
Another organization (not partner or competitor)	1%
Competitor	1%
Customer (B2C)	1%
Unknown	45%

Origin of external agents by percent of breaches within External



Who brought down Scarface?



Alfonso Capone



“The Secret Six has licked the rackets,. They’ve licked me. They’ve made it so there’s no money in the game.”

Recent Notable Successes

THE WALL STREET JOURNAL

DOW JONES
A NEWS CORPORATION COMPANY

TUESDAY, AUGUST 18, 2009 - VOL. CCLIV NO. 41

★★ \$3.00

DJIA 9135.34 ▼ 186.06 -2.0% NASDAQ 1930.84 ▼ 2.8% NIKKEI 10268.61 ▼ 3.1% DJ STOXX 50 2281.63 ▼ 1.9% 10-YR TREAS ▲ 18/32, yield 3.491% OIL \$66.75 ▼ \$0.76 GOLD \$934.30 ▼ \$12.70 EURO \$1.4083 YEN 94.44

What's News—

Business & Finance

World-Wide

Stock markets fell worldwide, shaking off recent optimism amid concern for the sustainability of a nascent global recovery. China's Shanghai Composite posted its biggest daily percentage drop since November. Japan's Nikkei had its worst day since March. European and U.S. stocks followed, with the Dow Jones Industrial Average losing 186.06 points, or 2%, to 9135.34. AI, CI, C2

Commodity futures fell as traders, losing faith in a con-

Prosecutors indict three in the largest cybercrime case. Albert Gonzales of Miami and two Russian accomplices were charged with masterminding a global scheme to steal data from more than 130 million credit and debit cards by hacking into the computer systems of five companies. AI

Wire fraud, all of which is now conducted in cyberspace due to Internet wire transfers, has exploded in recent years.

A suicide bomber attacked a police station in southern

Arrest in Epic Cyber Crime

A 28-Year-Old Allegedly Stole 130 Million Card Numbers; 'Get Rich or Die Tryin'

By SIOBHAN GORMAN

A 28-year-old American, believed by prosecutors to be one of the nation's cybercrime kingpins, was indicted Monday along with two Russian accomplices on charges that they carried out the largest computer hacking and identity-theft caper in U.S. history.

Federal prosecutors alleged the three masterminded a global scheme to steal data from more than 130 million credit and debit cards by hacking into the com-

puter systems of five major companies, including Heartland Payment Systems, Hannaford Bros. supermarkets and 7-Eleven.

The indictment in federal district court in New Jersey marks the latest and largest in nearly a decade of crime that has brought its alleged mastermind, Albert Gonzalez of Miami, in and out of federal grasp. Detained in 2004, Mr. Gonzalez was briefly an informant to the Secret Service before he allegedly returned to commit even larger crimes.

Authorities have previously

alleged that Mr. Gonzalez was the ringleader of a data breach that siphoned off more than 40 million credit-card numbers from the TJX Cos. and others last year, costing the parent company of the TJ Maxx retail chain \$200 million.

Mr. Gonzalez is currently in federal custody in New York, awaiting trial for his alleged efforts to hack into the computer network of the national restaurant chain Dave & Busters Inc.

The alleged thefts in Mon-



Albert Gonzalez

ISACA[®]
Trust in, and value from, information systems.
Jeddah Chapter

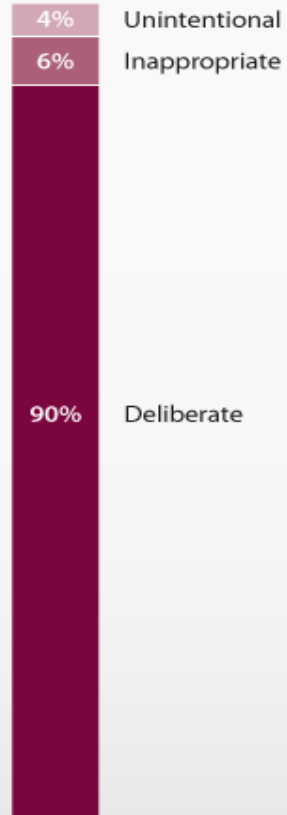


Slide 16

Thinking Beyond Ordinary

Internal Agents

Role of internal agents
by percent of breaches
within Internal

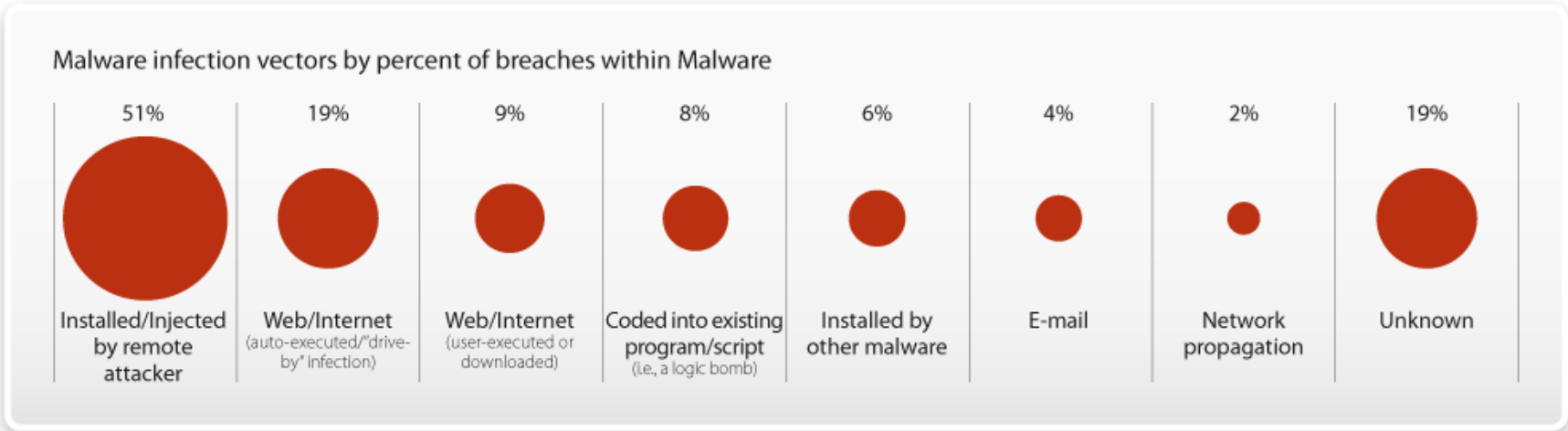


Types of internal agents by percent
of breaches within Internal

Regular employee/end-user	51%
Finance/accounting staff	12%
System/network administrator	12%
Executive/upper management	7%
Helpdesk staff	4%
Software developer	3%
Auditor	1%
Unknown	9%

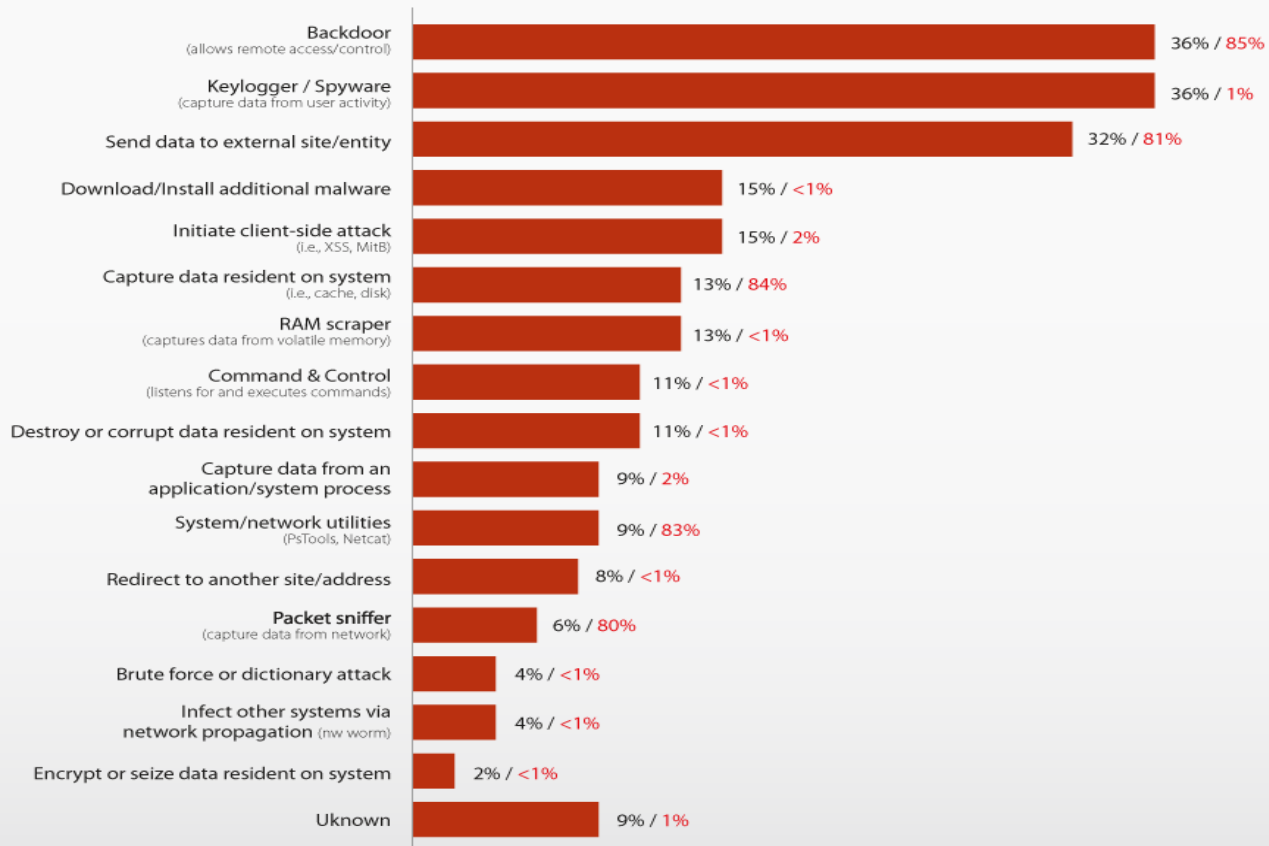
Malware

Infection Vector



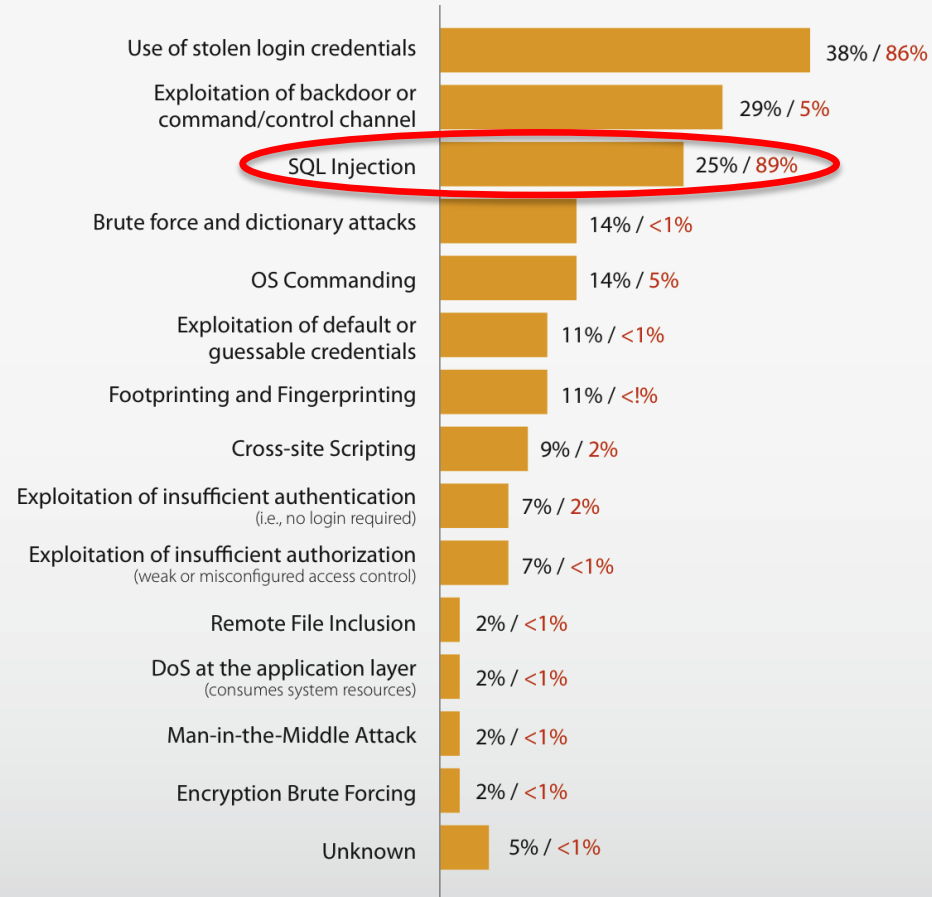
Malware Functionality

Malware functionality by percent of breaches within Malware and percent of records



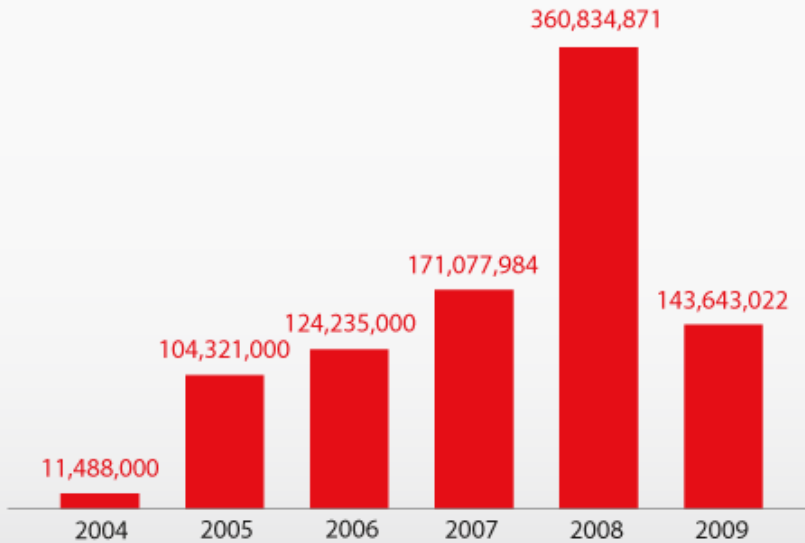
Hacking Types

Figure 21. Types of hacking by percent of breaches within Hacking and percent of records



Assets & Data

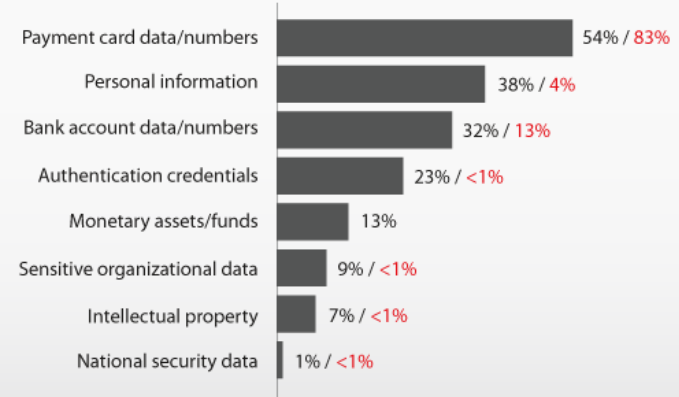
Number of records compromised per year in breaches investigated by Verizon and the United States Secret Service



Categories of compromised assets by percent of breaches and percent of records



Compromised data types by percent of breaches and percent of records



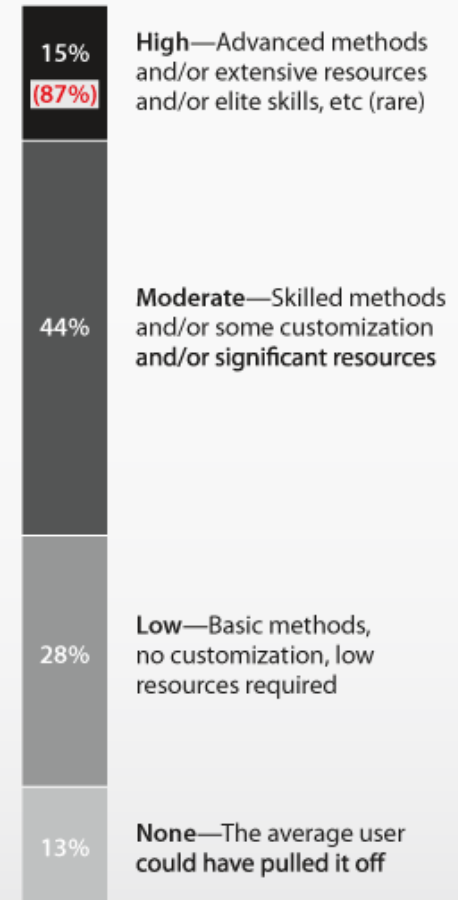
Attack Difficulty & Targeting

Attack targeting by percent of breaches **and records***



* Verizon caseload only

Attack difficulty by percent of breaches **and records***



* Verizon caseload only

Media & Press

Telegraph.co.uk

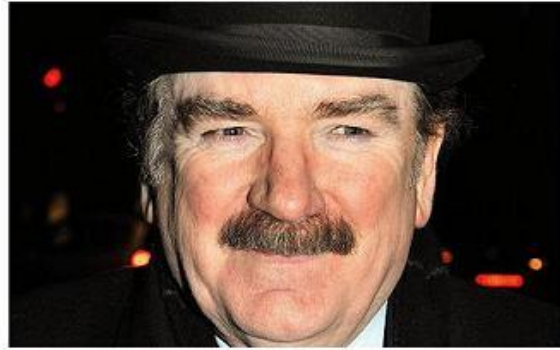
- Home
- News
- Sport
- Finance
- Comment
- Travel
- Lifestyle
- Culture
- Faith
- UK
- World
- Politics
- Celebrities
- Obituaries
- Weird
- Earth
- Science
- Health News
- Education
- Labour
- Conservative
- Liberal Democrats
- UK Politics Video
- US Politics Video

HOME > NEWS > NEWS TOPICS > POLITICS > LAW AND ORDER

'Lord of Fraud' convicted of plotting world's largest ever bank raid

A self-styled peer nicknamed the "Lord of Fraud" has been convicted of plotting to carry out the world's largest ever bank raid.

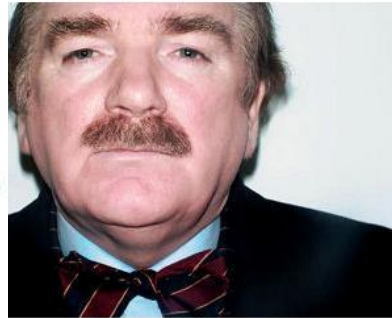
By Richard Edwards, Crime Correspondent
Last Updated: 8:37PM GMT 04 Mar 2009



Hugh Rodley, 'Lord of Fraud' convicted of plotting world's largest ever bank raid. Photo: PA

- T
- Email this article
- Print this article
- Share this article
- delicious
- Digg
- Facebook
- Fark
- Google
- Newsvine
- Reddit
- StumbleUpon
- Yahoo! Buzz
- Mix
- Twitter
- What are these?

LOOKING FOR A PREMIUM BANKING SERVICE TO HELP WITH YOUR BUSY LIFE?



Two guilty of £229m fraud attempt

Updated 07.07 Thu Mar 05 2009

Keywords: web, robbery, Sumitomo Mitsui Banking Corporation, david nash, hugh rodley, japanese, bank

A self-styled lord and a sex shop boss have been convicted over a "bold and sophisticated" bid to pull off the world's biggest theft.

Tensions are based on a manorial title, teamed up with a gang of web raiders targeting £229 million at Japanese financial giant Sumitomo Mitsui Banking Corporation.



TIMES ONLINE

- MONEY
- SPORT
- LIFE & STYLE
- TRAVEL
- DRIVING
- TECH
- ENVIRONMENT
- WEATHER
- TECH & WEB
- VIDEO
- PHOTO
- UK News
- Crime News

Hugh Rodley tried to pull off bank raid



- TIMES RECOMMENDS
- > Great Escape PoWs remember lost comrades
 - > Death of Hughes not Plath 'drove son to suicide'
 - > Rude names are dying from embarrassment

JS\$ 422 milhões de banco

ma/0_0489681-EI294_00.html

-未遂、440億円狙う・英紙

Sumitomo bank raid

7/sumitomo_cyber-heist_foiled/

BACK TO CRIME TOP

British man found guilty of plotting to defraud Japanese bank

Thursday 05th March, 06:45 AM JST



Sumitomo Mitsui "hackers" go on trial

Accused failed to fill out electronic transfer forms correctly, court told

Written by Tom Young
Computing 23 Jan 2009



A security supervisor helped the hackers into the building

attempt by criminal hackers to use banking group in the City, it

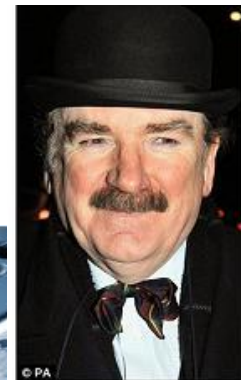
Card hacker'

EXPLORE UK NEWS

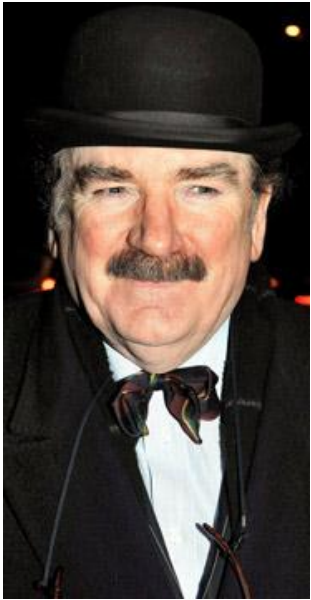
- > CRIME NEWS
- > EDUCATION NEWS
- > HEALTH NEWS
- > SCIENCE NEWS
- > SCOTLAND NEWS

TIMES RECOMMENDS

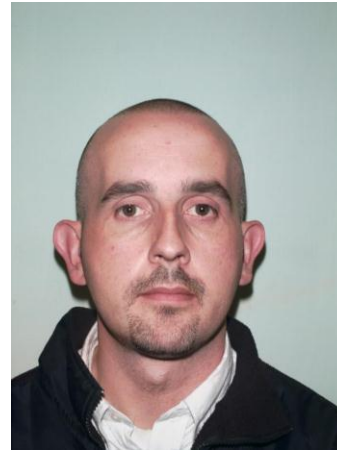
- > 'Great Escape' PoWs remember lost comrades
- > Death of Hughes not Plath 'drove son to suicide'
- > Rude names are dying from embarrassment



Convictions



Hugh Rodley
16 Years
£1.73m
Confiscation



Kevin O'Donoghue
4 Years 4 Months



Jan Van Osselaer
3 Years 6 Months



David Nash
3 Years

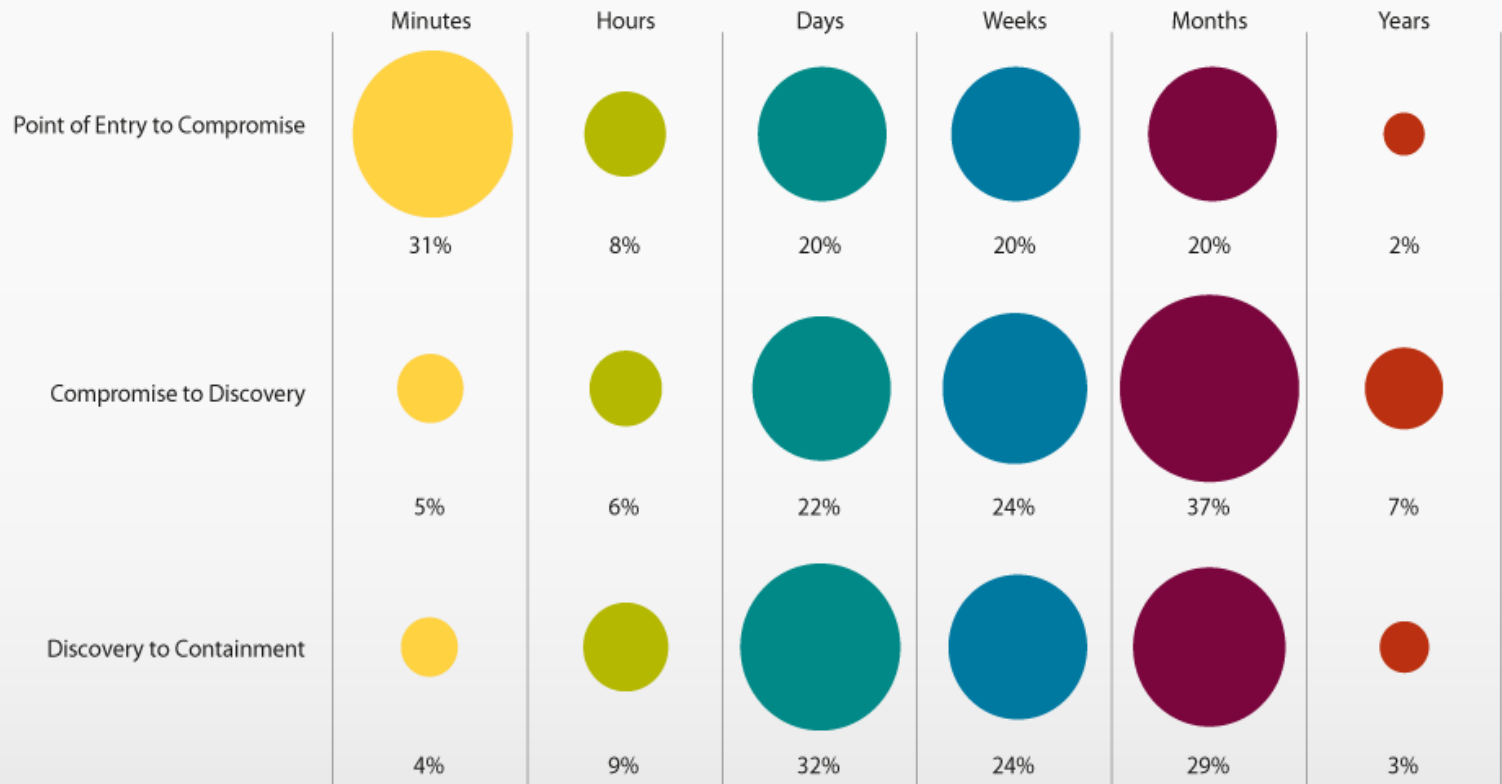


Gilles Poelvoorde
4 Years



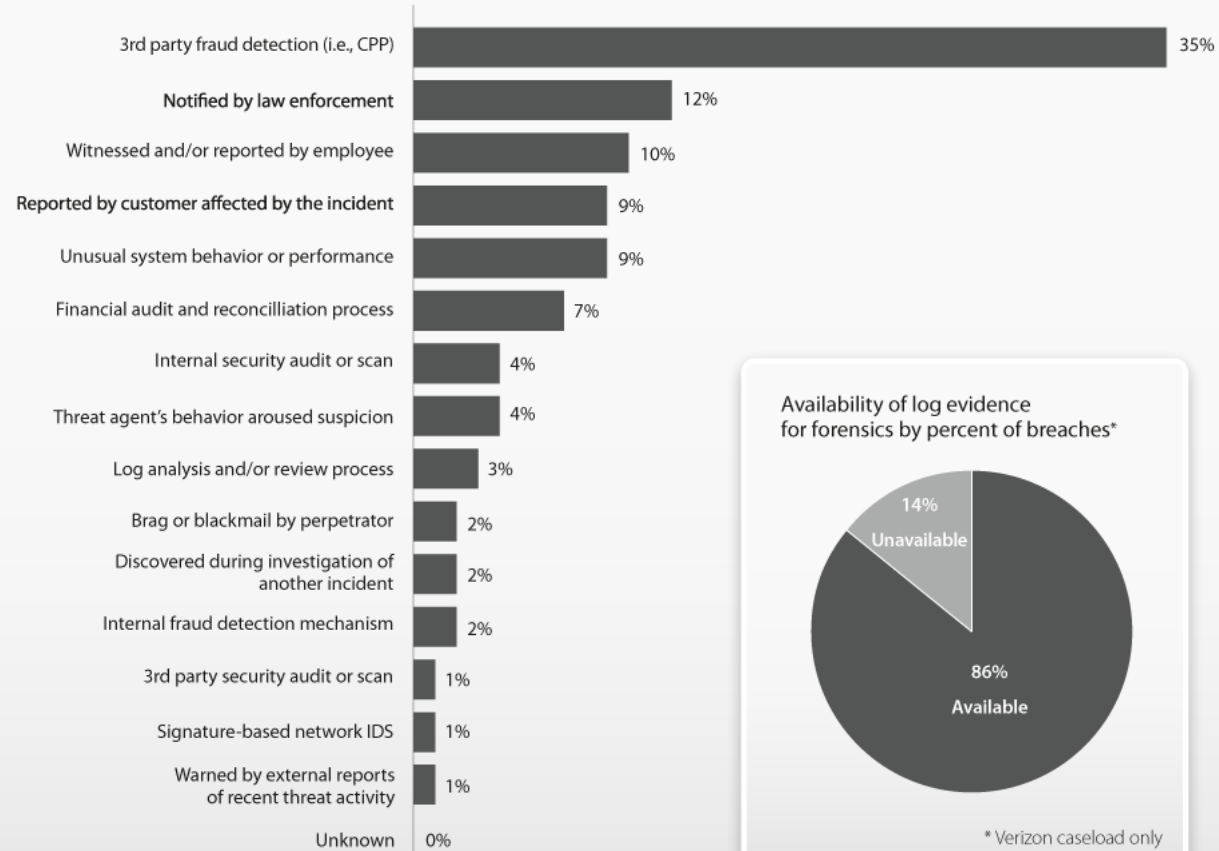
Time Span of Events

Timespan of events by percent of breaches

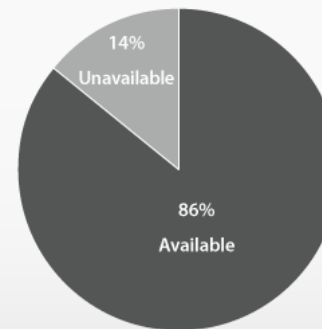


Discovery Methods

Breach discovery methods by percent of breaches



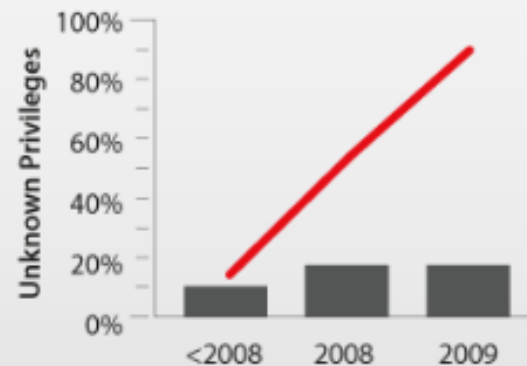
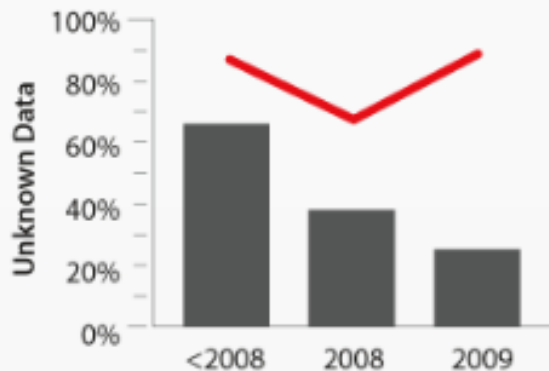
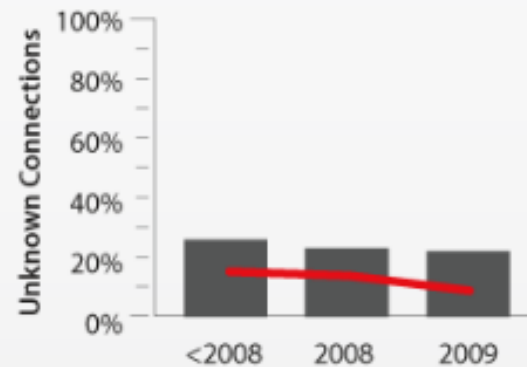
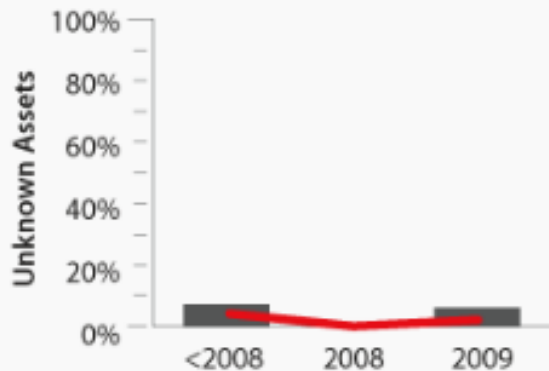
Availability of log evidence for forensics by percent of breaches*



* Verizon caseload only

Unknown Unknowns

Unknown Unknowns by percent of breaches and percent of records



PCI DSS

Percent of relevant organizations in compliance with PCI DSS requirements based on post-breach reviews conducted by Verizon IR team*

	2008	2009
Build and Maintain a Secure Network		
Requirement 1: Install and maintain a firewall configuration to protect data	30%	35%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	49%	30%
Protect Cardholder Data		
Requirement 3: Protect Stored Data	11%	30%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	68%	90%
Maintain a Vulnerability Management Program		
Requirement 5: Use and regularly update anti-virus software	62%	53%
Requirement 6: Develop and maintain secure systems and applications	5%	21%
Implement Strong Access Control Measures		
Requirement 7: Restrict access to data by business need-to-know	24%	30%
Requirement 8: Assign a unique ID to each person with computer access	19%	35%
Requirement 9: Restrict physical access to cardholder data	43%	58%
Regularly Monitor and Test Networks		
Requirement 10: Track and monitor all access to network resources and cardholder data	5%	30%
Requirement 11: Regularly test security systems and processes	14%	25%
Maintain an Information Security Policy		
Requirement 12: Maintain a policy that addresses information security	14%	40%

PCI DSS compliance status based on last assessment*



* Verizon caseload only

* Verizon caseload only

Conclusion & Recommendations

Overall

- USSS cases afforded more complete picture of breaches
 - Further confirmation on what we already observed
 - New insight from pieces of the picture we were missing

Agents

- External small majority of breaches, dominates overall data loss
- Largely due to organized crime
- Internal up because of USSS cases
- Partner down again in both datasets

Actions

- Two most-common scenarios
 - Exploit error, gain access to network/systems, install malware (External)
 - Exploit privilege, abuse access and/or embezzle funds/data (Internal)
 - Still not highly difficult or targeted though slightly more than before

Conclusion & Recommendations

Assets

- Most data compromised from servers & apps
- Desktops/laptops increasing; related to stolen credentials
- Most criminals interested in cashable forms of data

Discovery & Response

- Discovery still takes a long time and is largely due to third parties
- Response and containment slow and prone to mishap

Mitigation

- The basics – if done consistently – are sufficient in most cases
- Keep outsiders out; they are increasingly difficult to control once in
- Restrict and monitor insiders; disable access when they leave
- Maintain adequate resources for detection; make better use of logs
- Plan, prepare, train, and test for a timely and effective response
- e-Crime Prevention and good IT Security

Remember

- **Partnerships**
- **e-Crime Prevention**
- **Education, Education, Education**
- **e-Voids**
- **Digital Intelligence**

