Fraud & Risk Detection in Government

Deborah Pianko, Principal - SAS Security Intelligence

THE POWER TO KNOW.

But I have great employees.
They would never do that.

Rita Crundwell - $54 Million over 22 years

Dixon, Illinois Comptroller

Largest municipal fraud in U.S. history.

Praised by officials for “(looking after) every tax dollar as if it was her own.”

- Secret bank account
- Wrote checks from the fund payable to "Treasurer," which she would deposit into account.
- In 1991, she stole $181,000, while in 2008 alone she managed to embezzle $5.8 million.
- Bought horses, several cars, a second house and a million-dollar motorhome
- She had an $80,000 city salary
- Used money to support horse breeding business

Harriette Walters - $48 Million over 20 years

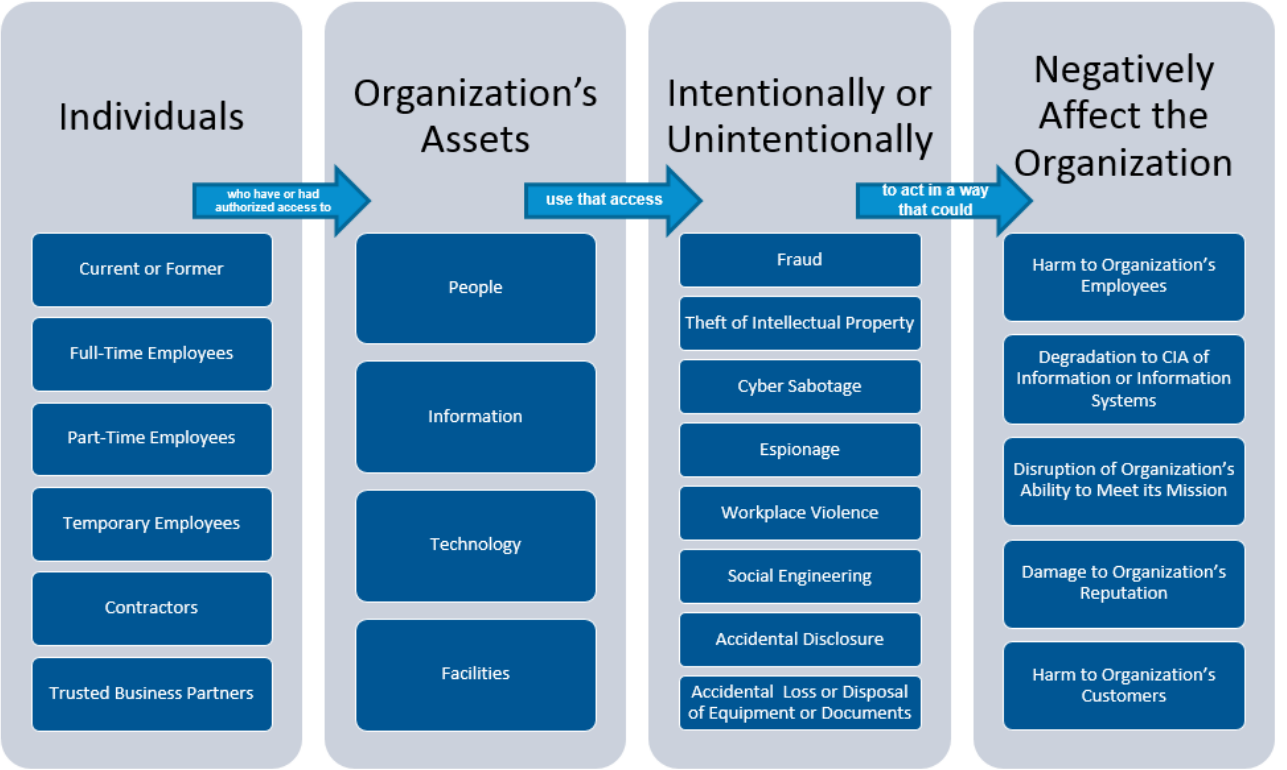
D.C. Office of Tax & Revenue – Manager, Real Property Tax Division

Walters used her position at OTR to create false property tax refund vouchers that produced millions of dollars of fraudulent refund checks. From June 1989 through August 2007.

- Shopping sprees at Nordstom, Neiman Marcus - $2.3 million
- Designer purse - $25K
- 45 trips to Las Vegas and Atlantic City
- Cash and checks to co-workers $1.2million

Who and What is an Insider Threat - Prioritizing

What do you want to protect, and from whom?



There is Not One Type of Insider Threat

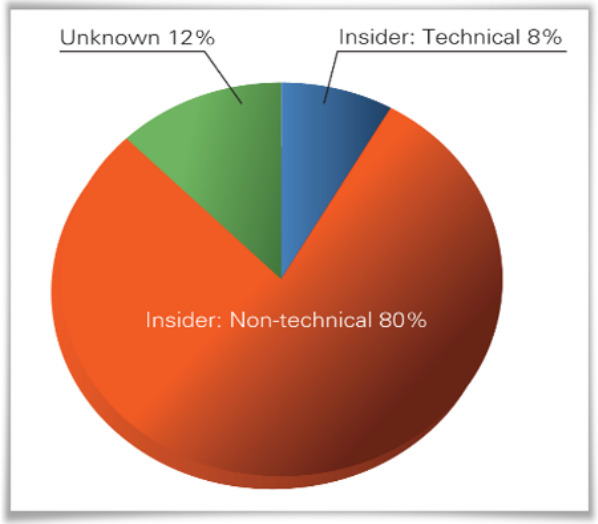
3 Behavioral Profiles – IT Saboteur, Financial Fraudster and IP Thief

	IT Sabotage	**Fraud**	**Theft of Intellectual Property**
Current or former Employee?	Former; disgruntled	Current; stressed	Current (within 30 days of resignation); can be disgruntled but not necessarily
Type of position	Technical (e.g., sys admins, programmers, DBAs)	Non-technical (e.g., data entry, customer service) or their managers	Technical (e.g., scientists, programmers, engineers) or sales
Gender	Male	Fairly equally split between male and female	Male
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) or Customer Information
Access Used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At Work

Low Tech

Methods are detectable

Insiders' means were not very technically sophisticated.

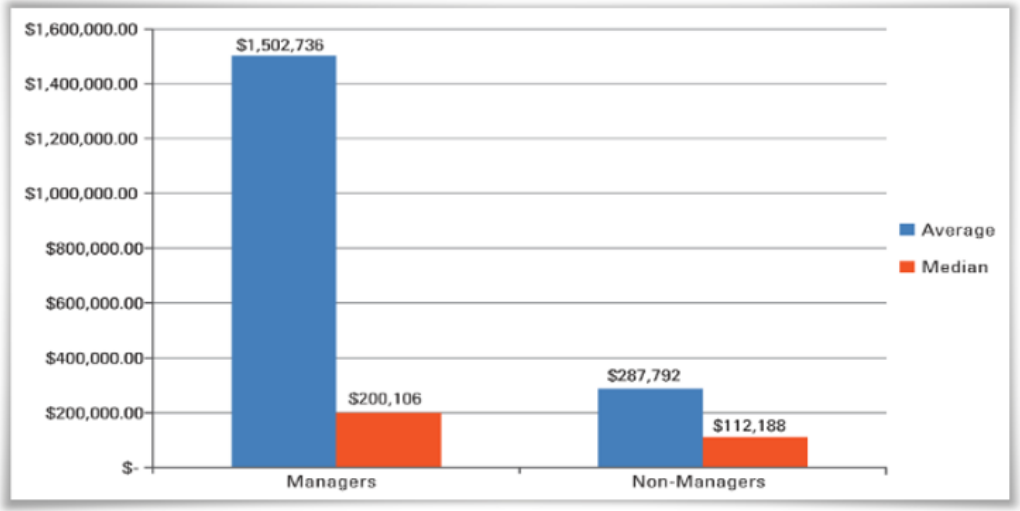


Non-technical subjects were responsible for 65 (81 percent) incidents. Seven were external attackers, but their methods were also non-technical.

Managers vs. Non-Managers

Managers are more trusted – but do more harm

Fraud by managers differs substantially from fraud by non-managers by damage and duration.

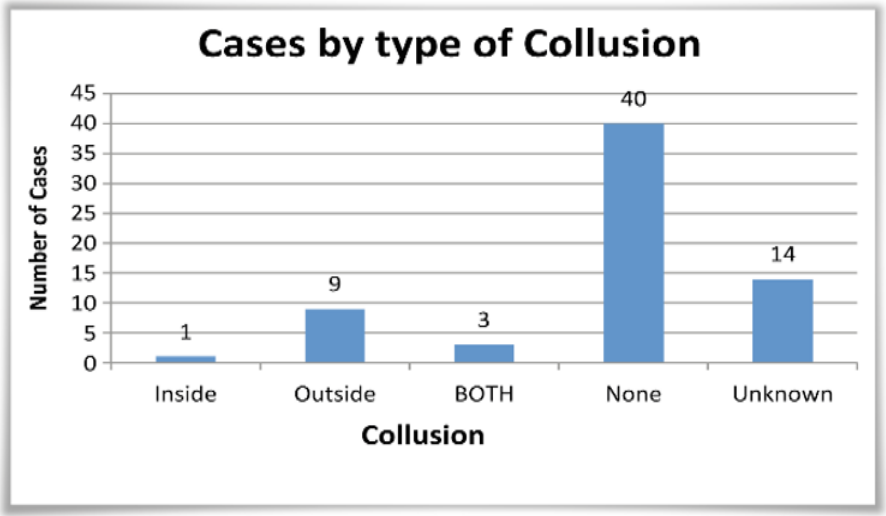


Of 61 subjects, 31 (51 percent) were managers, VPs, bank officers, or supervisors. The median results show that managers consistently caused more actual damage ($200,106) than non-managers ($112,188).

Collusion

With exception of a certain type of IP Thief (The “Ring Leader”)

Most cases do not involve collusion.



There was not a significant number of cases involving collusion, but those that did occur generally involved external collusion (i.e., a bank insider colluding with an external party to facilitate the crime).

Statistics are human beings with the tears wiped off.
-Paul Brodeur, *Outrageous Misconduct*

Insider Threat – 2016 Statistics

- Forty-seven percent (47%) of survey participants reported that an insider incident was committed against their organization.

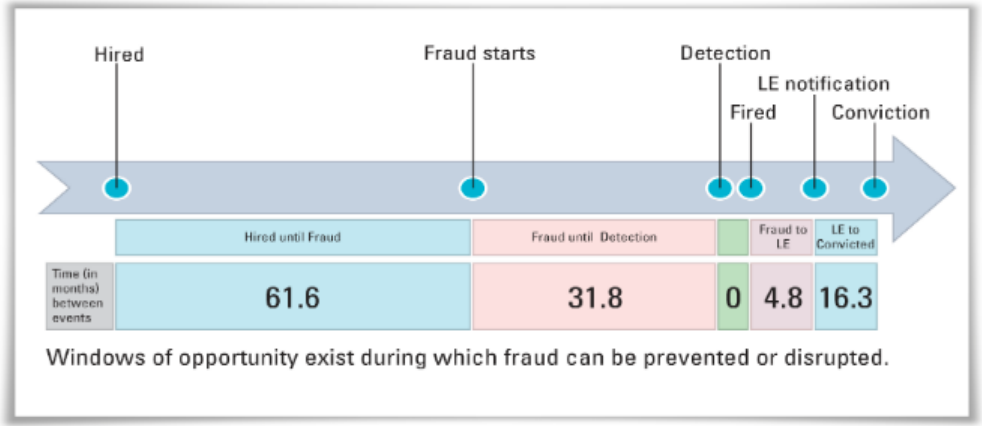
- More than one in four (27%) of all attacks against their organization were committed by insiders

- The most common insider incidents were customer records compromised or stolen, confidential records (trade secrets or intellectual property) compromised or stolen, and private or sensitive information was unintentionally exposed.

Insider Threat Detection & Continuous Monitoring

Dwell Time - Low and Slow

Prevention may be possible through better onboarding, but earlier detection is key



There are, on average, over 5 years between a subject's hiring and the start of the fraud.

There are typically 32 months between the beginning of the fraud and its detection.

Criminals who executed a "low and slow" approach accomplished more damage and escaped detection for longer.

- Ongoing reinvestigation/regular monitoring after hire
- Termination and departure monitoring
- Employee awareness and path to report unusual behavior

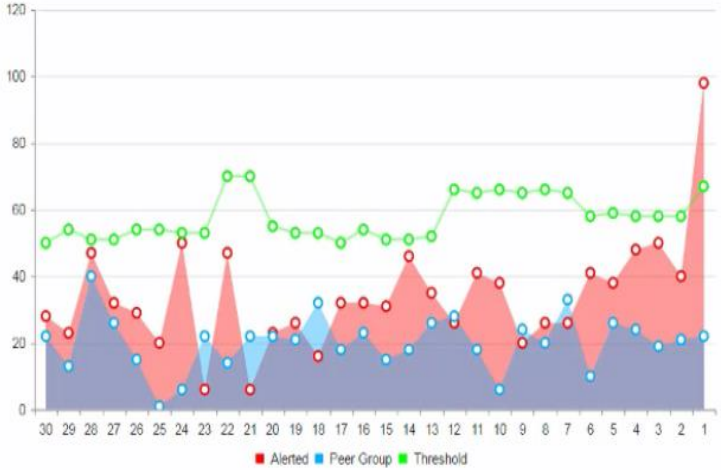
Examples of Detection Approaches

- File downloads which are excessive for the employee's peer group
- Atypical privileged account access (e.g. VIP taxpayers)
- Abnormal viewing/modification of taxpayer accounts (or lack thereof)
- Analysis of web activity
- Sentiments (i.e. feelings) expressed in work email or instant messages that are highly correlated with insider threat
- Unusual time-of-day access
- Employees' connections and sphere of influence in the organization
- Printer activity
- Use of external media devices
- Override of technology settings
- Monitoring of database queries and/or copying
- Data exfiltration monitoring (e.g. plagiarism detection)

The Quest for Defining Normal – Peer Group Comparison

Alert Details | Risk Summary | E-Communications | Time Of Day Access | Network

Daily Risk Scores with Peer Group Comparison



High Risk Activities Timeline

Risk Factors

Da	Risk Factor Descript...	Risk Factor Score	Mac...	Risk Fact...
Dec 7, 2015	Excessive Uploads(Size and/or Frequency)	20	Primary	Exces. File Upld
Dec				

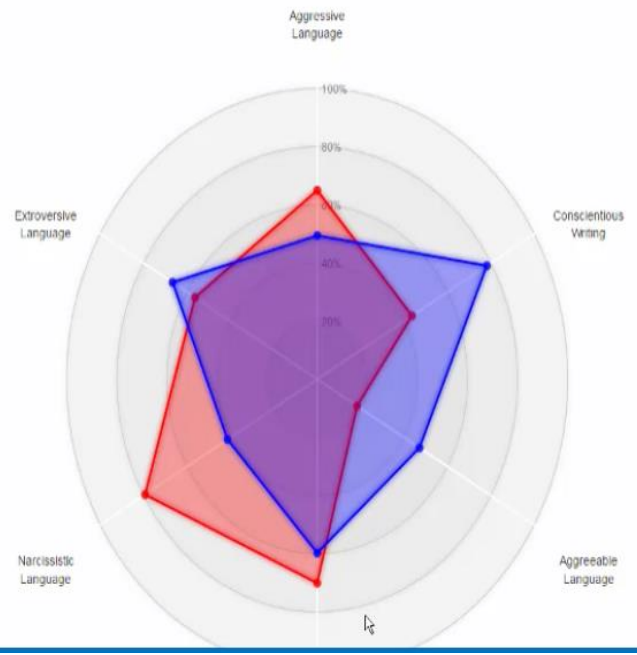
Associated Co-Workers

co_worker	department	role	score

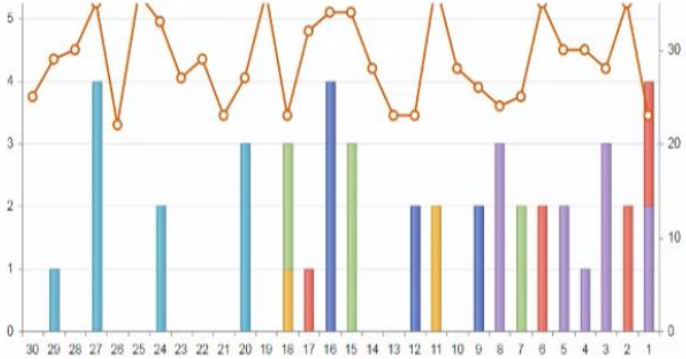
The Quest for Defining Normal – Unstructured Data

Alert Details | Risk Summary | E-Communications | Time Of Day Access | Network | +

Writing Style Comparison



E-Communications Topics of Interest



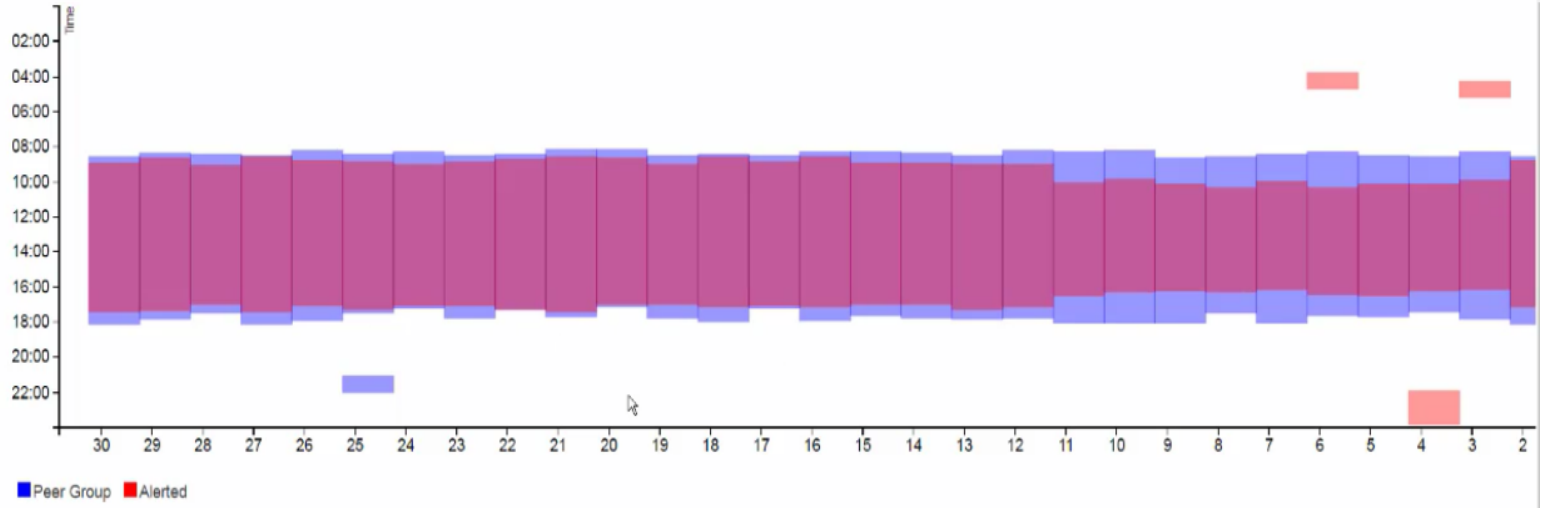
Email Contents - Disgruntled (2016-01-19)

Dat...	To	BC	Contents
Jan 19, 2016	To...		My manager is the root cause that every one of us here suffers. He is the best politician I have ever seen in my life. Ever since he promoted to be a manager, he started to play all the dirty games among us. Not these junks... how does it happen? pick ur guess! How about we go the manger above him. Too bad.. the upper manager is his buddy. There is no complain or any bad thing would ever leak out through these 2 layers of managers. They cover everything up very well. In fact, one of the manager as jobs should ensure the fairness

The Quest for Defining Normal – Time of Day Access

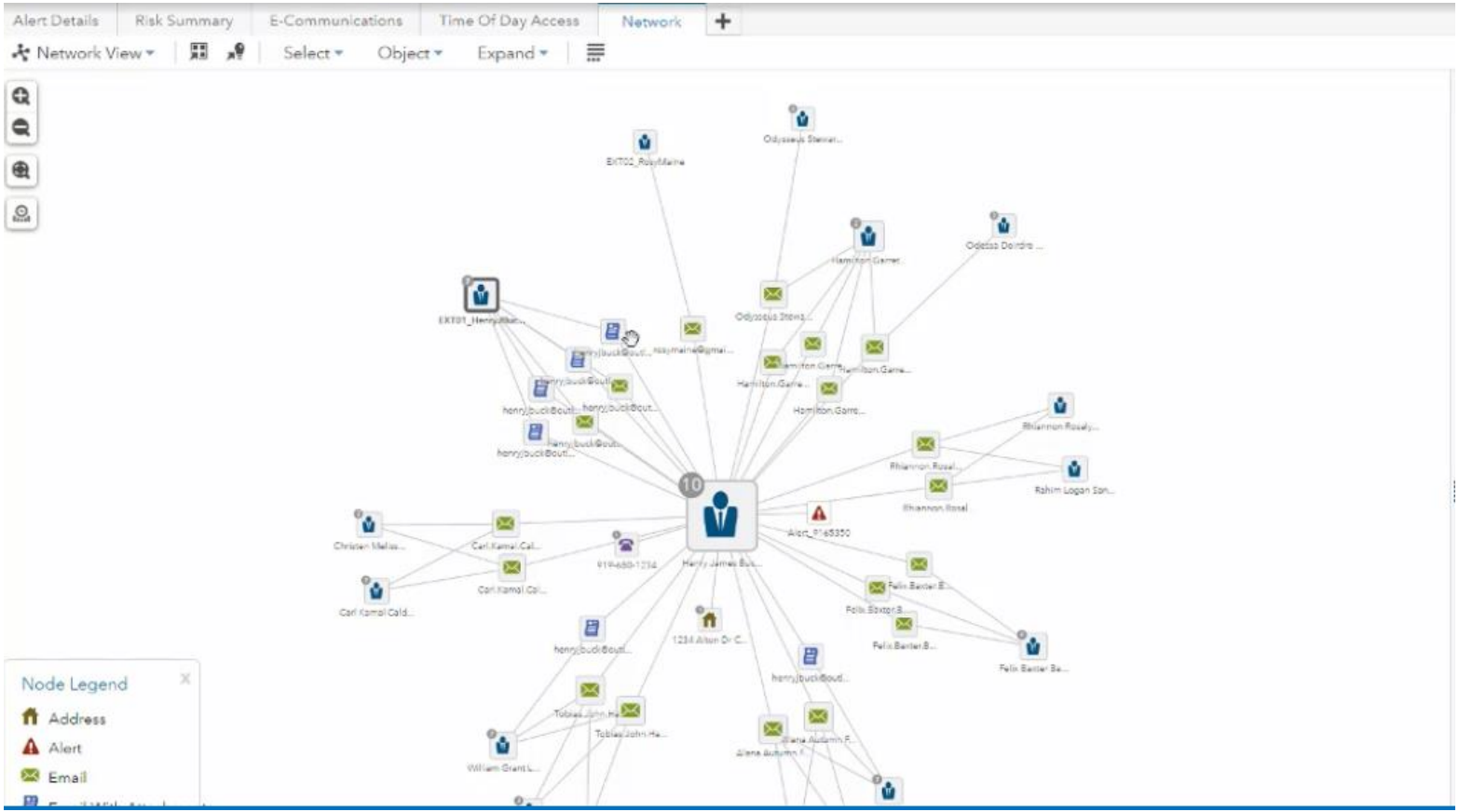
Alert Details | Risk Summary | E-Communications | Time Of Day Access | Network

Time of Day Access



Day	Date	Owner	PC	Service	Ticket
1	2016-01-19	ALR0766 - Armando Lucas Rivas	pc-2769	Apply OS Patches	AK190
1	2016-01-19	KFM0249 - Kamal Forrest Miranda	pc-2495	Deploy Software - gpo	DSG7-
1	2016-01-19	DBJ3716 - Driscoll Beau Jefferson	pc-9925	Configure Disk Partition	U9L1-5
1	2016-01-19	NJM2246 - Nicolas Jarrod Morton	pc-1208		

The Quest for Defining Normal – Relationships



The Lines are Blurry

Defense in Depth Required

"The best way to get into an unprepared company is to sprinkle infected USB sticks with the company's logo around the car park."

DSM

https://hbr.org/2014/09/the-danger-from-within

Tax Evasion

TAX AGENCY CHALLENGES / SAS AREAS OF EXPERTISE

Identity Theft

Analysis of Complex Structures (e.g Passthroughs)

Tax Evasion

Underreporting, Non-Filers and Stop-Filers

Audit Selection & Success Prediction

Insider Threat Detection & Cybersecurity

Debt Collections Optimization

Economic Forecasting

Crime Ring/Network-Level Detection & Relationship Visualization

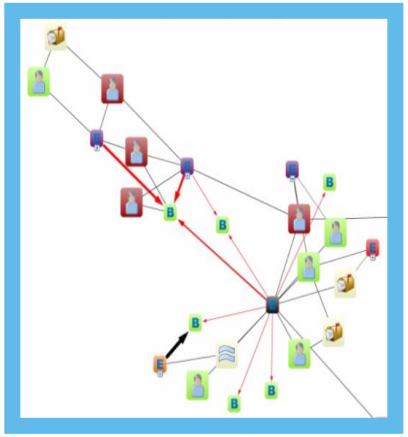
Data Aggregation

Ad-hoc Data Mining

Business Intelligence

SAS® Tax Clients

- U.S. IRS
- Kentucky
- Iowa
- North Carolina
- South Carolina
- Louisiana
- Ireland
- Belgium
- Australia
- United Kingdom
- Netherlands
- Singapore
- Sweden
- Italy
- Estonia
- Spain
- India
- Mexico
- Canary Islands
- Saudi Arabia



Highlights

- VAT carousel fraud reduced by 98% (from 1.1 billion € to 0.029 billion €)
- Ultra-early detection
- SAS hybrid approach provides a high accuracy model (80% true positive rate)

FPS FINANCE (BELGIUM), VAT Carousels

Business Problem

Organized VAT Fraud was a billion euro problem for the Belgian Government. This fraud typology is a high velocity fraud: “Carousel frauds are like floods. It is futile to believe that after the storm we can put back water in the riverbed with buckets. What is needed is to build dykes to prevent overflows” .

SAS Approach

The solution is used to detect **companies with a high probability of being involved in Organized VAT Fraud**. The SAS Hybrid approach provides ultra-early detection from the first suspect VAT return or other suspicious behaviour. This Hybrid approach combines network analysis, business rules, predictive modeling and anomaly detection. The combination of these methods enables new networks to be discovered and to monitor known networks. The models are highly accurate (80% true positive rate). This makes the SAS Hybrid approach the ideal tax auditor.

Results

The result is a **reduction by 98% (from 1.1 billion € to 0.029 billion €) of the VAT carousel fraud**. Analytics was key in achieving this result. **The models are not only very accurate (80% true positive rates),** they also provide **ultra-early detection** as from the first VAT declaration. Organized VAT fraud is now a controlled phenomenon. The system also enables international collaboration by identifying suspicious companies abroad.

SERIOUS & ORGANISED VAT FRAUD

VAT CAROUSEL

Offshore

220,000 VAT stolen

Belgium

France

Conduit Company (A)

VAT-Free

1,000,000 Cost

0 VAT

Missing Trader (B)

VAT

1,100,000 Cost

220,000 VAT

Buffer Company (C)

French Treasury

Gets only 20,000 VAT from Company C

V A T

1,200,000 Cost

240,000 VAT

Profit Taker (D)

VAT-Free

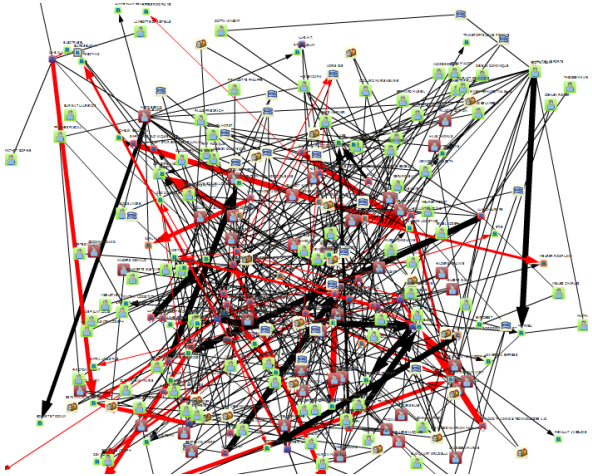
Goods never actually have to leave the dock in France

May recycle same goods many times through ("carousel")

Or can sell to totally different company in another EU country (e.g. Germany) – not always back to original company

Detection Techniques

THE BEST TECHNIQUE IS MULTIPLE TECHNIQUES

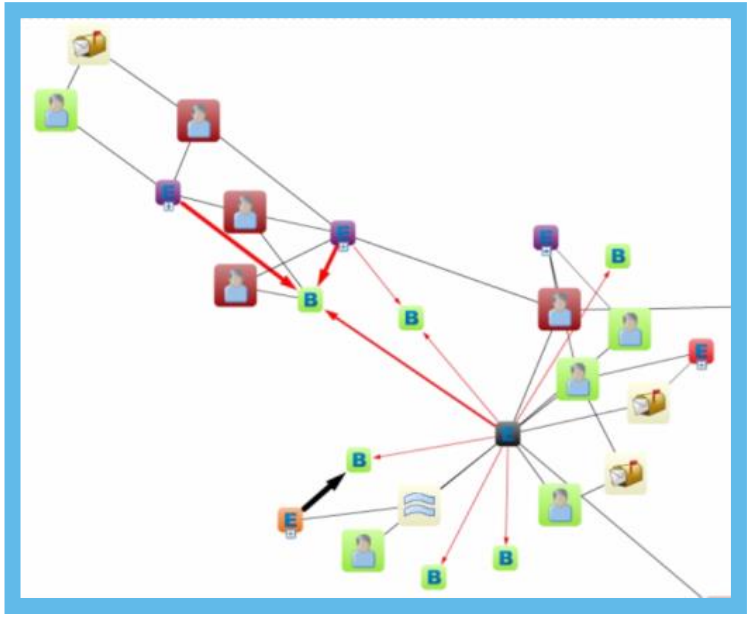


$$Q = \frac{1}{2w} \sum_{(u,v)\in A} \left(w_{uv} - \frac{w_u w_v}{2w} \right) \Delta(c_u, c_v)$$

$$w = \sum_{(u,v)\in A} w_{uv}$$

$$w_u = \sum_{v\in\delta_u} w_{uv}$$

- SAS® Social Network Analysis
  - Network Analytics
  - Network Scoring
- Anomaly Detection
- Predictive Modeling
- Business Rules
- Fuzzy Matching



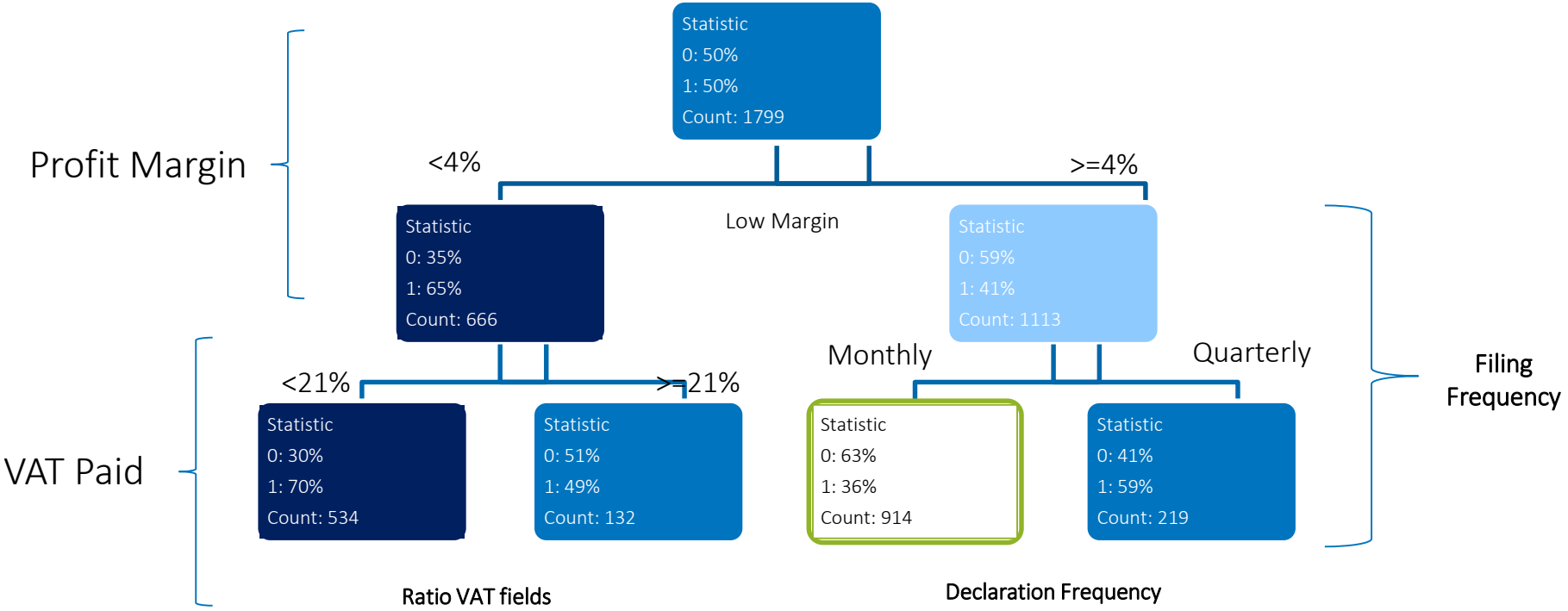
- Louvain algorithm
- Reach (Ego) networks
- Shortest path

Detection Techniques

WHAT ARE WE LOOKING FOR

- Common network structures and activity between nodes that have shown in past to correlate with fraud (e.g. money flow, VAT return data, claims for refunds)
- Relationships to risky entities (measures of closeness, between-ness, etc.)
- Reduction of supercluster down to it's key components (fuzzy matching)
- Predictive modeling – Have we seen this before?
- Anomaly/outlier detection – Does this entity act like it's peers?

BUFFER COMPANY
Decision Tree



Fuzzy Matching

REDUCING THE SUPERCLUSTER

John Smith	13/01/1980	18 Queen Street	JN 12 34 56 A
John Smith	13/01/1980		
J. Smith	13/01/1980	18 Queen Street	0208 123 45676
John Smythe			JN 12 34 56 A
Smith	13/01/1980		0208 123 45676

DataFlux Data Management Studio 2.5

2 NYS Tax - Match Sample MDAS Data

File Edit View Actions Tools Window Help

2 NYS Tax - Match Sample MDAS Data

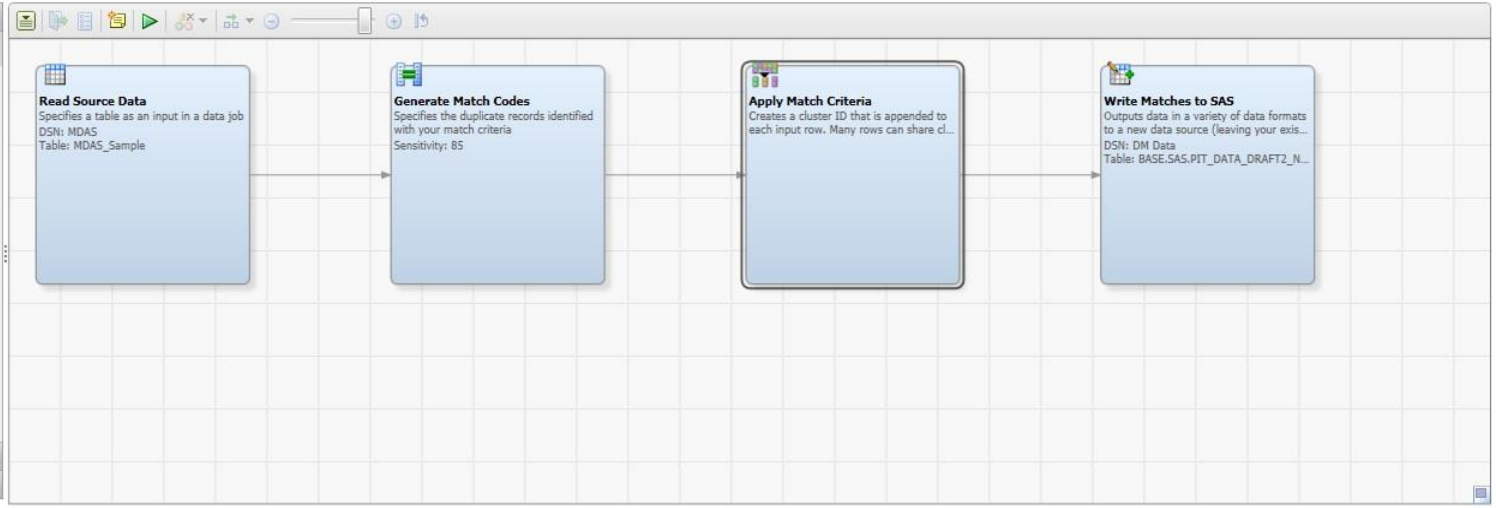
Data Flow | Settings | Variables | Log

Nodes

- Data Job
- Data Inputs
- Data Outputs
- Data Integration
- Quality
- Enrichment
- Entity Resolution
- Monitor
- Profile
- Utilities

Folders

Accelerators



Basic Settings | Advanced Properties | Preview | Node Connections | Log

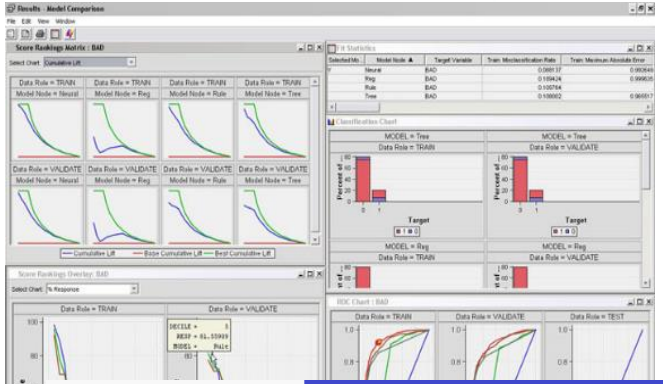
Apply Match Criteria

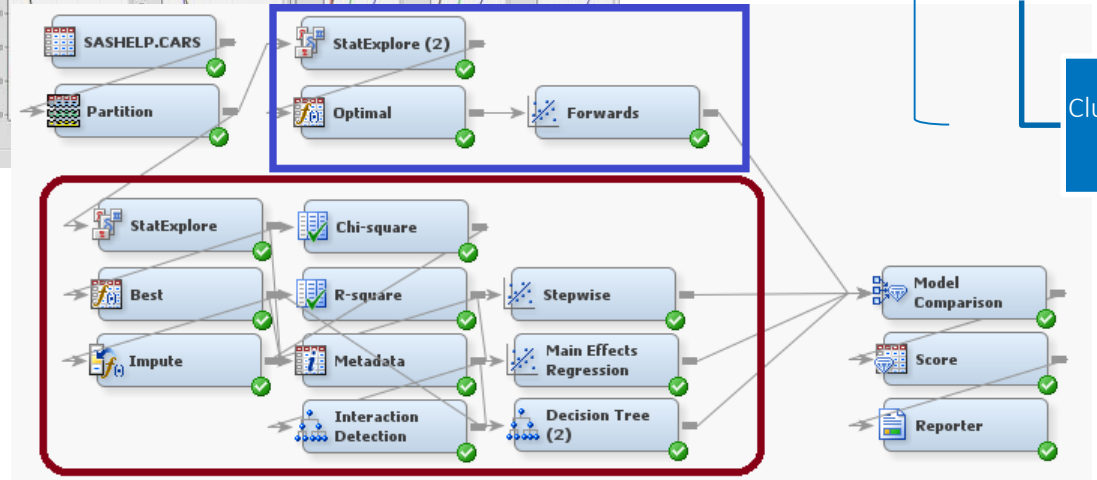
View Value...

	State	Zip	TAX_ID	NAME_LEGAL	STREET	CITY	FILER_FREQ_CD	ORIG_BBNY_DT	TERM_RSN_CD	TERM_RSN_DESC	TERRITORY_CD	AUDIT_AVAILABILITY	NAME_LEGAL_MC	CLUSTER_ID
1	NY	10307	690922657	The Learning Tree	7299 AMBOY RD	STATEN ISLAND	A	6/1/1989 12:00:00 AM			BAQ	Y	W££YP£PF~Y_$$$$$$$$$$$$$$$$$$$$$$$$	0
2	NY	10307	690922657	The Learrning Trees	7299 AMBOY RD	STATEN ISLAND	A	6/1/1989 12:00:00 AM			BAQ	Y	W££YP£PF~Y_$$$$$$$$$$$$$$$$$$$$$$$$	0
3	NY	10307	185772816	Ferniture Fixer	7254 AMBOY RD	STATEN ISLAND	Q	3/1/1983 12:00:00 AM			ECD	Y	G£YP£~£Y_G£X£Y$$$$$$$$$$$$$$$$$$$$$$	1
4	NY	10307	185772816	Furniture Fixers	7254 AMBOY RD	STATEN ISLAND	Q	3/1/1983 12:00:00 AM			ECD	Y	G£YP£~£Y_G£X£Y$$$$$$$$$$$$$$$$$$$$$$	1
5	NY	10307	265178387	NEI Michael	46 MAIN STREET	STATEN ISLAND	A	11/1/2010 12:00:00 AM			BAQ	Y	P_7B73_$$$$$$$$$$$$$$$$$$$$$$$$$$$$	2
6	NY	10307	265178387	Nei michaels	44 MAIN STREET	STATEN ISLAND	A	11/1/2010 12:00:00 AM			BAQ	Y	P_7B73_$$$$$$$$$$$$$$$$$$$$$$$$$$$$	2
7	NY	10307	111111111	TGI Fridays Inc	5373 ARTHUR KILL ROAD	STATEN ISLAND	Q	9/30/2004 12:00:00 AM			ECD	Y	~F7GY£8£R$$$$$$$$$$$$$$$$$$$$$$$$$$	3
8	NY	10307	172473316	TGI Friday's	5373 ARTHUR KIL ROAD	STATEN ISLAND	Q	9/30/2004 12:00:00 AM			ECD	Y	~F7GY£8£R$$$$$$$$$$$$$$$$$$$$$$$$$$	3

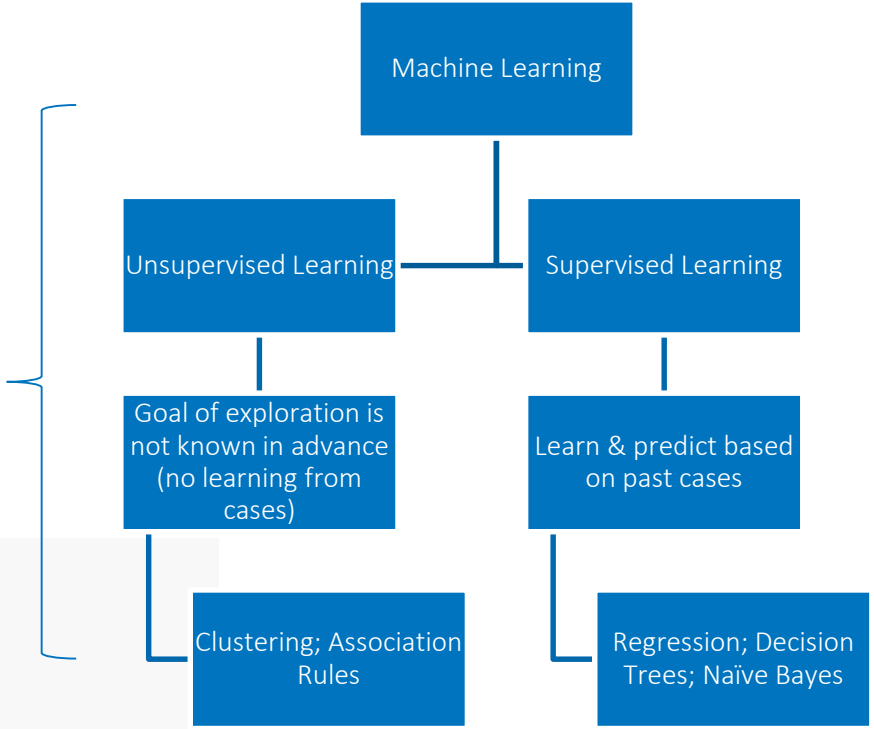
Job Status:

Machine Learning





Different techniques depending on the goal of the modeling exercise



More fish in same holes?
Or find new holes to fish in?

Home Alerts Tasks Search | 9435805494 × | 19682873199 ×

Close Immediately | 0 Comment

Alert Details | Return Details | External Data | Triggers | Scoring History | Alert History | Workspace-1 | +

Scenario Information

Scorecard 935

Feb 2, 2017 5:14:00 AM

2016 5337889

Taxpayer Profile Identity Theft Model	420
Change in Deduction and Preparer Use	205
Significant Change in Filing Date	110
IP Address Out of State and Refund > $500	100
Employer Wage Report Mismatch	100

Employer **Miller LLP** reported wage differs from wages on tax return by **10%** or more. This return shows a variance of **$40,226** / **45%** .

Taxpayers

Person (1)

Name	Person ID
Barbara Baez	240430804

Details

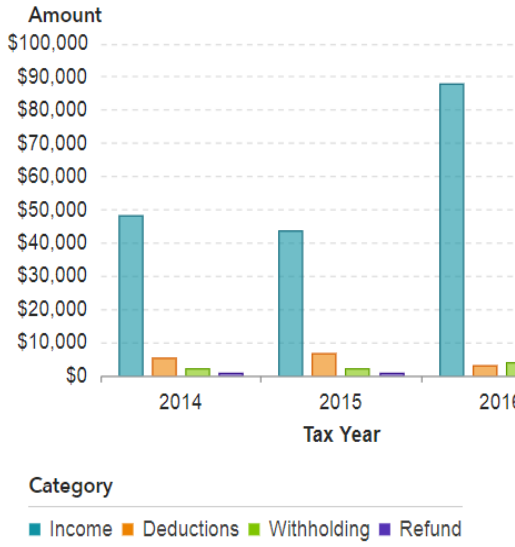
Person ID
240430804

Address
66 Prospect Hill St

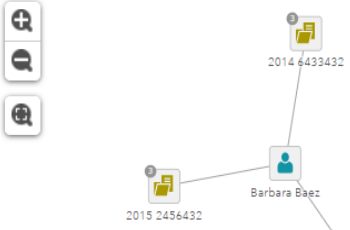
City
Newport

Zip
02840

Tax Overview | Neighborhood Map | Model Scorecard



Network



Return Summary

Income Tax Return (3)

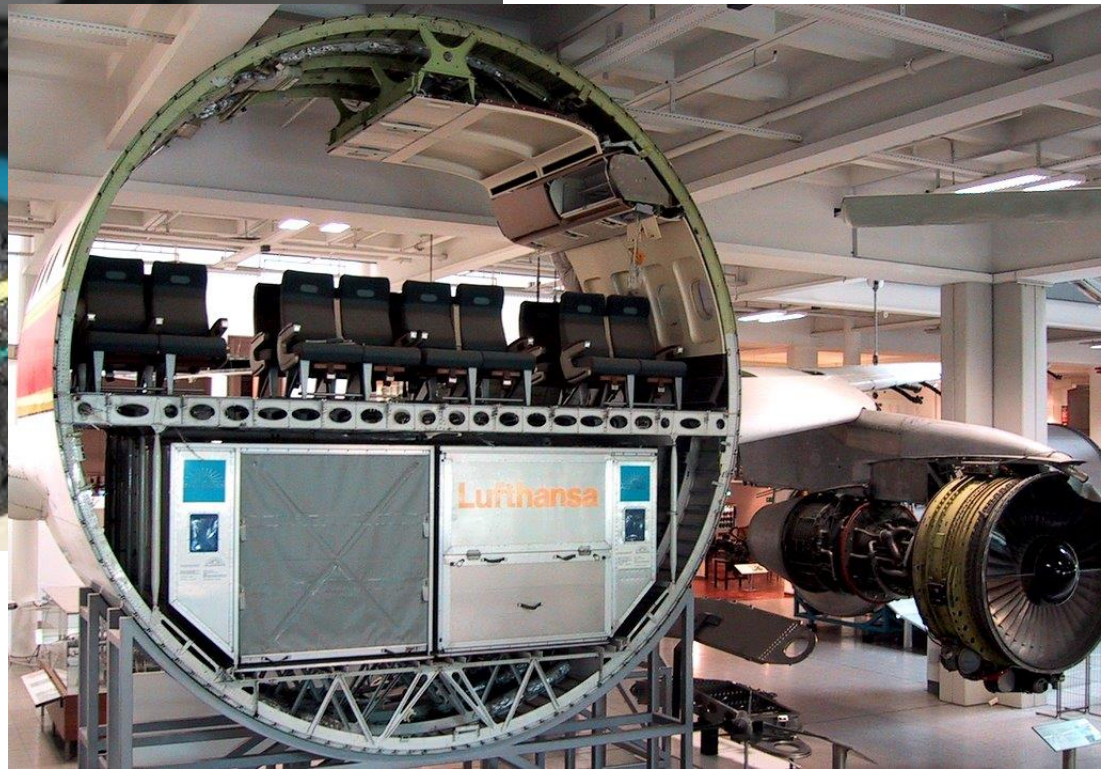
Tax Year	Return D...	Filing Sta...	Deduction	Refund	Bank Acc...	IP Addre
2014	Mar 27, 2015	Married Joi	Itemized	$844	0530 009162	73.98.26

Customs & Border Control

Yemen incident 2010

Two bombs headed to U.S., intercepted in Dubai and the UK and defused

Failed attempt to sabotage cargo aircraft using explosives hidden in printer cartridges



Found after a tip-off from Saudi authorities; may have been test packages before

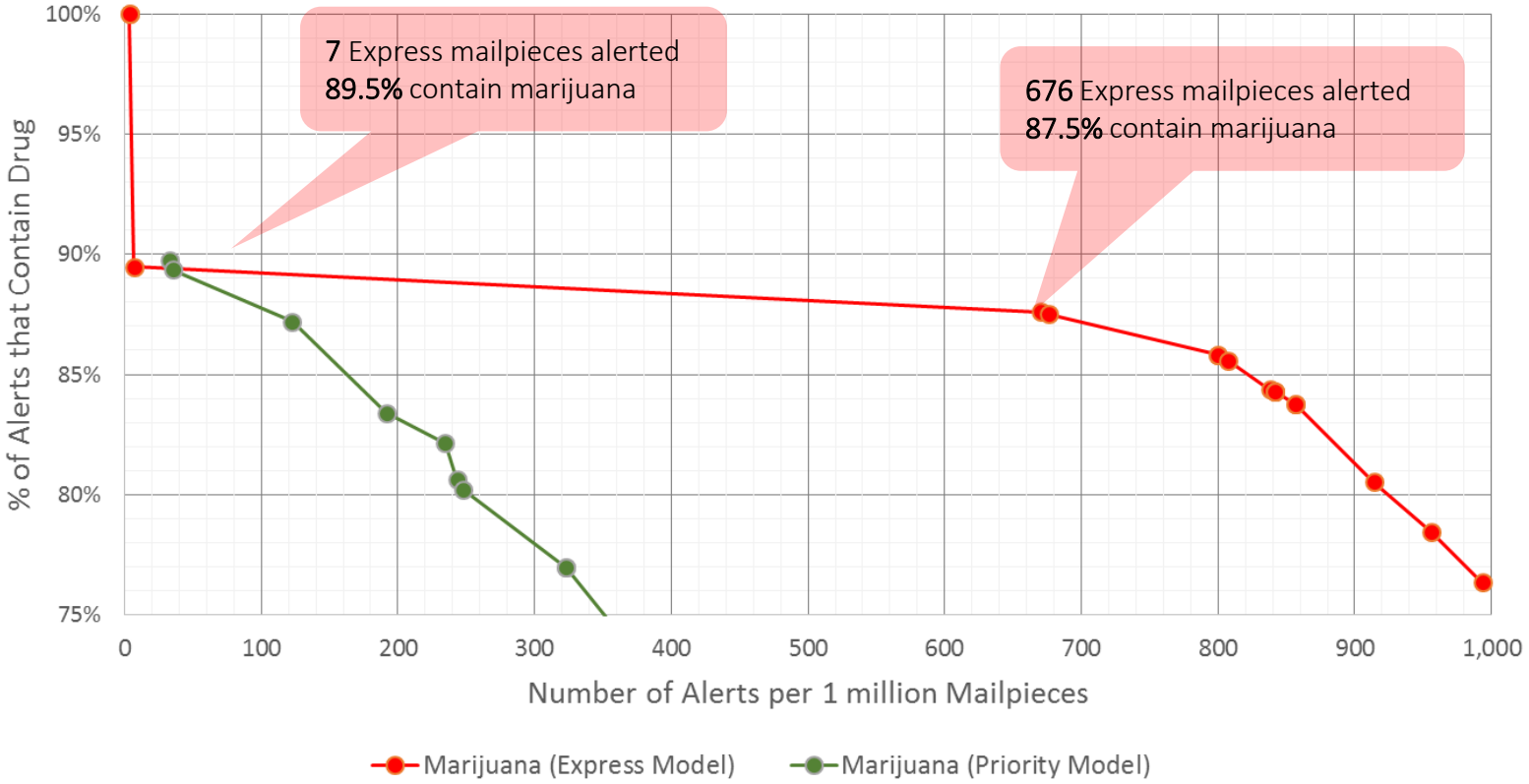
Types of Fraud

CUSTOMS

- Drugs
- Tobacco
- Alcoholic beverages
- CITES
- Intellectual property rights (IPR) - Counterfeiting
- Precursors
- Tax and duty evasion
- Weapons and explosives
- Currency
- Nuclear materials
- Hazardous material
- Pornography / Paedophilia
- Other prohibitions and restrictions (including works of art, stolen vehicles, anabolic steroids etc.)

Tradeoff between Number of Alerts and Precision

US POSTAL MARIJUANA MAILPIECE TARGETING



Notes:
1) assume marijuana mailpieces make up 0.133% of all mailpieces
2) assume mail class of marijuana mailpieces are 62% Express, 38% Priority

Fraud Dual Use

- What are Dual-Use commodities?
  - Goods and technologies are considered to be dual-use when they can be used for both civil and military purposes.
  - Most industrialized countries have export controls on dual-use goods

Problem:

Chlorine is a dual-use item, both pool supply companies and terrorists might want to make use of it. But how to distinguish between the two?

Solution:

Identify rules to 1) detect export companies not declaring dual-use items 2) detect unusual patterns of export.

- Nuclear
- Chemicals
- Electronics
- Computers
- Lasers
- Sensors
- Marine
- Avionics
- Propulsion

Fraud Dual Use

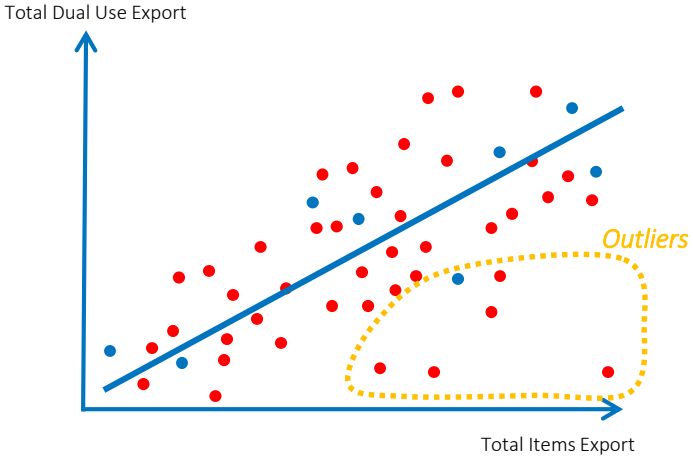
ANOMALY DETECTION USING MARKET BASKET ANALYSIS

IF *3917 – Tubes, Pipes and Hoses* *AND* (*3926 – Other Plastics* *OR* *85 - Electrical Machinery*)

THEN

4016930000 - Gaskets

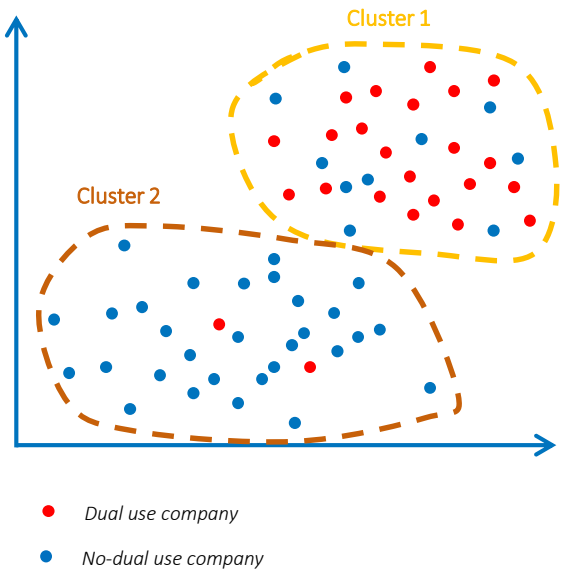
- Basket analysis of all commodities exported by dual-use companies
- Find Associations between dual-use and other commodities - Identify strong and interesting associations
- Extrapolate to all export companies and look at their dual-use exports



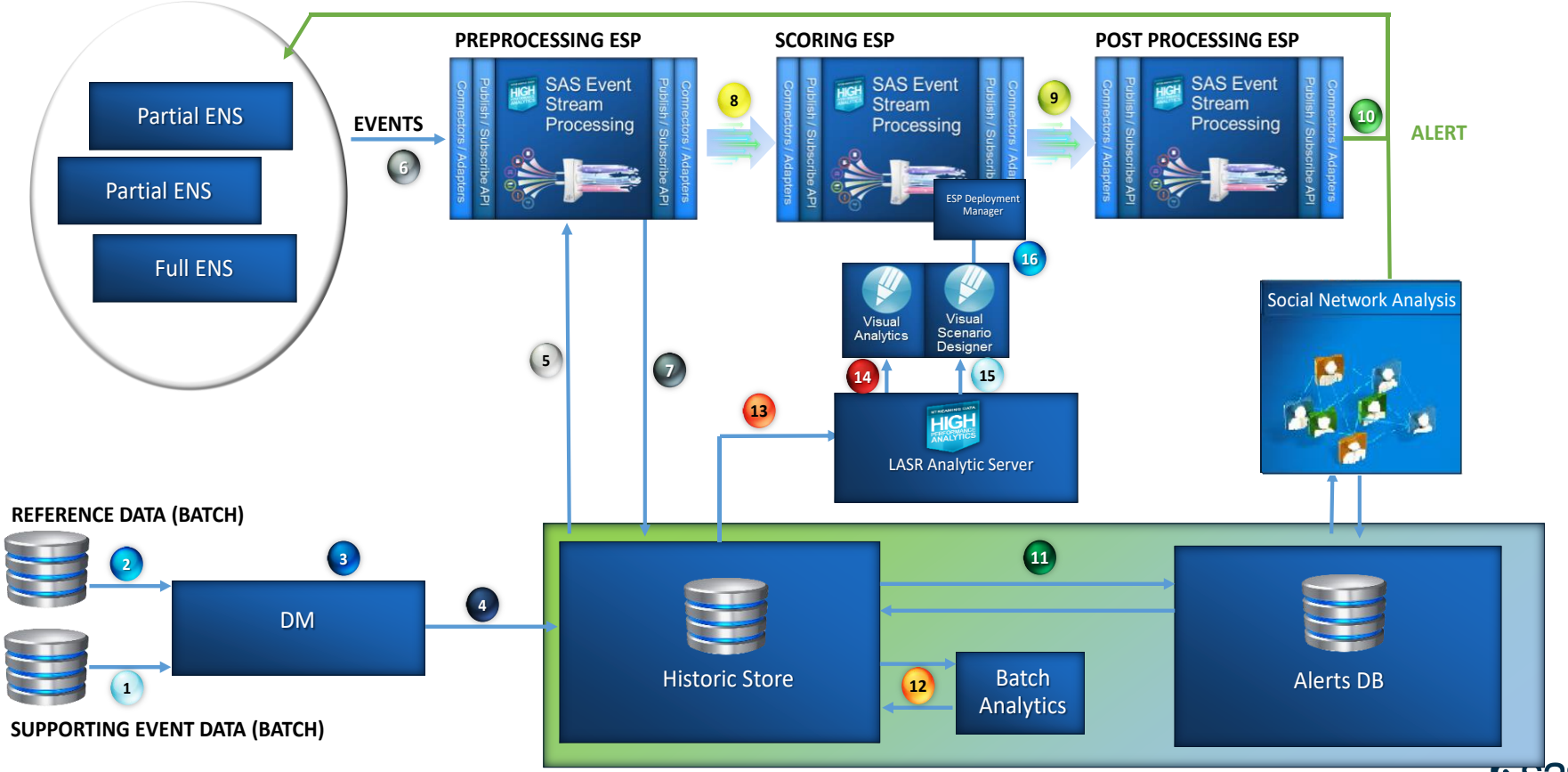
Fraud Dual Use

ANOMALY DETECTION USING CLUSTERING

- Profile companies exporting dual use vs. other companies
  - Export in a lot of countries
  - Export commodities in group 85 (electrical machinery) and 84 (nuclear reactors)
  - Big exporters
  - Mainly road transport
  - Also export 73 (Iron/Steel), 90 (Optical) and 39 (Plastics)
- Look at similar companies which aren't exporting dual use commodities
  - 370 companies with similar profile



Real-time deployment



Thank You