IBM
FRAUD ÇÖZÜMLERİ

13 Mart 2014

Incomplete view of criminal networks and patterns limits recoveries and prosecution rates

What We've Heard:

"No analytics today on multiple investigative requests or for commonalities between current and past patterns"

"Today we can't detect identity theft schemes…the common denominators are hidden to us"

Technology Barriers:

- Fragmented transactional and security data sources / no master database
- Limited data search and analysis tools for investigators

Enabling Capabilities:

- Enterprise intelligence repository for collaboration
- Rapid, powerful Information Analytics
- Investigator control of data gathering and report generation
- Alerting functionality makes team members aware of shared interest in an individual or group
- Web portal gives search access to external team members
- Detailed security options to protect data distribution
- Complete evidentiary material governance

Building

Benefit / Improvement Opportunities:

- Increase recoveries per case due to more complete view of linked criminal activities resulting in prosecution of larger networks with more assets for seizure
- Improve success rate due to inclusion of more complete body of relevant data, more powerful analytics, and responsiveness of law enforcement (LE)
  - Fresher data, use of LE terms/formats, and larger fraud networks means a better chance of pursuit and prosecution of the criminals
  - Improved collaboration and automatic alerts drive deeper insights leading to more successful cases

IBM

Investigative efficiency limits the ability to quickly close cases

What We've Heard:

*"Takes **'quite a while'** (eg, several hours) to search multiple different data systems"*

"Today each investigator determines when 'enough' information has been collected"

Technology Barriers:

- Fragmented transactional and security data sources / no master database
- Limited data search and analysis tools for investigators

Enabling Capabilities:

- Automate collection of data from specific data sources
- Investigators create own ad hoc federated searches across multiple data sources
- Predictive fraud analytics, entity resolution, link analysis, transactional analysis and geospatial analysis
- Complex algorithms for Social Network Analysis to better apply focus and resources
- Heat matrices, histograms, and filtering to quickly identify hidden relationships in the data

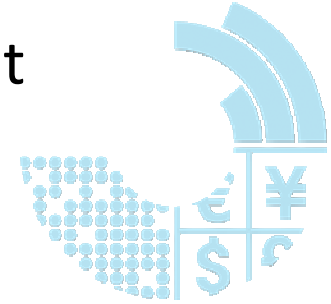
Benefit / Improvement Opportunities:

- Increase case capacity without adding resources due to ability to tie together multiple related cases into one and Improve overall case review and investigation times
- Reduce case cycle time due to faster turn around of investigation data improving team speed and efficiency
- Lower cost due to better data availability and more efficient collaboration (fewer resources working the same case)
- Better data accuracy and completeness without manual manipulation or multiple query attempts for the same information

Building t

IBM

Major Retailer: A 4.75-year manual investigation by Asset Protection Team leads to a single conviction…AFTER $1,000,000 in losses incurred due to one employee



In 2013, the investigation was simulated using i2 tools…

- Quotes from the IBM client:

  "I'm very upset…but in a good way. I used my source data from the nearly five-year investigation – but employed the i2 tools this time."

  "In under two hours I had the entire forensic picture visualized, evidence correlated, and bad actors identified."

  "I am convinced that if I had used i2 from the beginning, the case would have been solved in under two weeks and handed over to prosecution."

  - Asset Protection Investigative Analyst

- The retailer lost over $1M (USD) by working methodically, with manual methods
- Using i2 solution would have sped the process by over 120x, saving nearly $1M
- New discoveries for the retailer since visualizing the large case with i2:
  - Day 1: Retailer discovered possible collusion with other employees and vendors related to the 5-year case
  - Links discovered to organized rings involved with E-commerce frauds
    - Fraudsters shopping online with stolen credit cards
    - Mules pick up goods at store before stolen cards are flagged
    - Some merchandise was quickly fenced in small stores in low-income neighborhoods
    - Larger volumes of misappropriated goods fenced online or sold on the streets
    - Links pointing to complex suspected crime organizations; state and Federal LE engaged

IBM

Retail Use case example

Top 50* Retailer

- The challenge at this company has been to link all likely suspects to events and create a product to take to law enforcement
- Because of the high amount of theft at the stores, this company wanted to determine
  - if thefts were conducted by the same or different individuals
  - if the 'individuals' were actually part of a larger organized group
- By using IBM i2 the Central Investigation Team (CIT) provides quick and accurate analysis and visualization of common links by importing the thousands of spreadsheets that are gathered from store locations
- **Bottom line…**
  - Investigators are more productive
    - What used to take hours can now take minutes
    - More (and faster) discoveries and case resolutions per investigator
  - Investigations drive more prosecutions and recoveries
    - What used to look like one-off incidents can be identified as organized criminal activity
    - Law enforcement more responsive to recognizable data and reports, and to larger enterprises for prosecution

*According to Fortune Magazine's 2013 ranking of the 500 largest companies in the US (ie, the Fortune 500)

"Individual masterminds a three-year scheme that stole more than $600,000 from [major Retailer]"

- 49-year-old Robert Milton is in Mecklenburg County Jail, arrested for allegedly masterminding a three-year scheme that stole more than $600,000 from [a major Retailer] stores in three states, and put scores of investigators on his trail
- The take so far – $624,000 – is expected to grow as [the Retailer] tabulates further losses, the affidavit says.
- Hints of trouble…
  - Milton, who previously lived in Charlotte, Rock Hill, Fort Mill and Belmont, was first confronted on Dec. 29, 2010, when employees of a store in Monroe called police for what they thought was a fraudulent return of merchandise
  - No charges were filed, but a store investigator launched a probe into Milton's activities with the retail chain
  - Two years later, the same store investigator contacted [law enforcement] and asked that "numerous fraudulent returns/refunds" at stores across the Southeast be looked into

*The Charlotte Observer, May 2013

Customer theft and organized retail crime rose 13.4%

- 697,000 employees were apprehended in 2011 after having stolen $1,765 on average
- In total, employee or supplier theft and fraud, organized retail crime and administrative errors cost the U.S. retail industry $41.7 billion in 2011 (representing 1.6% in sales)[1]
  - $18.4 (44%) attributed to employee theft
  - $14.9 (36%) to shoplifters
  - $6.6 (16%) to internal errors
  - $1.8 (4%) in supplier fraud
- Customer theft and organized retail crime rose 13.4% in 2011 vs. 2010

[1] *Global Retail Theft Barometer,* Checkpoint Systems (2012)

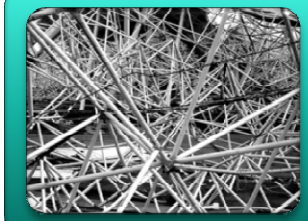
Organized Retail Crime and Loss Prevention: Billions and Billions Up for Grabs *(June 10, 2013 - 24/7 Wall St.)*

- The National Retail Federation puts the cost of organized retail crime to retailers at $30 billion a year
- 72% of retailers reported online reselling (eFencing) and fencing of items resold elsewhere happened to 69% of retailers
- A whopping 78% reported that they had been victims of gift card and store credit fraud. Top items: baby formula, laundry detergent, energy drinks, high-end denim, allergy medicine, and cell phones

*June 10, 2013 - 24/7 Wall St

Risk of fraud and financial crimes is growing

Fraud is on the rise



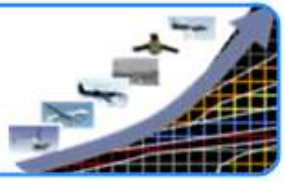
Becoming more complex

Traditional defenses are not sufficient

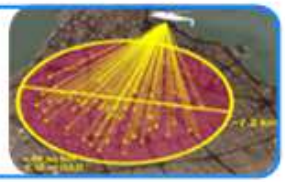
IBM

Data and internal organizational boundaries hide threats

V_1 Volume
- Available data
- Accessible sources



V_2 Variety
- Data types
- Analytical Methods



V_3 Velocity
- Data flow
- Decision making

V_4 Veracity
- Data accuracy
- Information integrity

The danger of not responding is significant

Direct impact

7% of revenue, growing 8% annually

?

Need?

Brand Damage

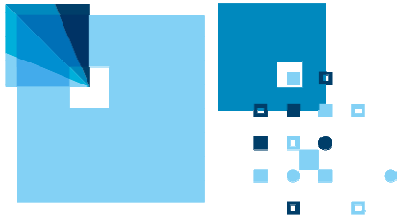
Lost customers; lost shareholder value

IBM

Converging forces are creating a heightened focus on fraud and financial crimes

12 Cyber crime victims **per second**[1]

80% originate in organized activity[4]



Schemes are increasing in complexity and frequency

The explosion in global connectivity has escalated the vulnerabilities of individuals, enterprises and nations to cyber crime.

$4.7 **trillion** Global cost of fraud today[2]

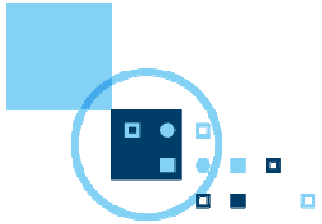
$1.92 billion fine in a money-laundering case[5]

Economic and societal costs of fraud have escalated

Intensified regulatory enforcement and operational losses apply significant pressure on profitability.

71% Customers who will switch banks because of fraud[3]

46% Customers leaving or avoiding a company with a security breach[6]



Customer expectations have intensified

Customer confidence and trust drive brand choice and must be earned on an ongoing basis.

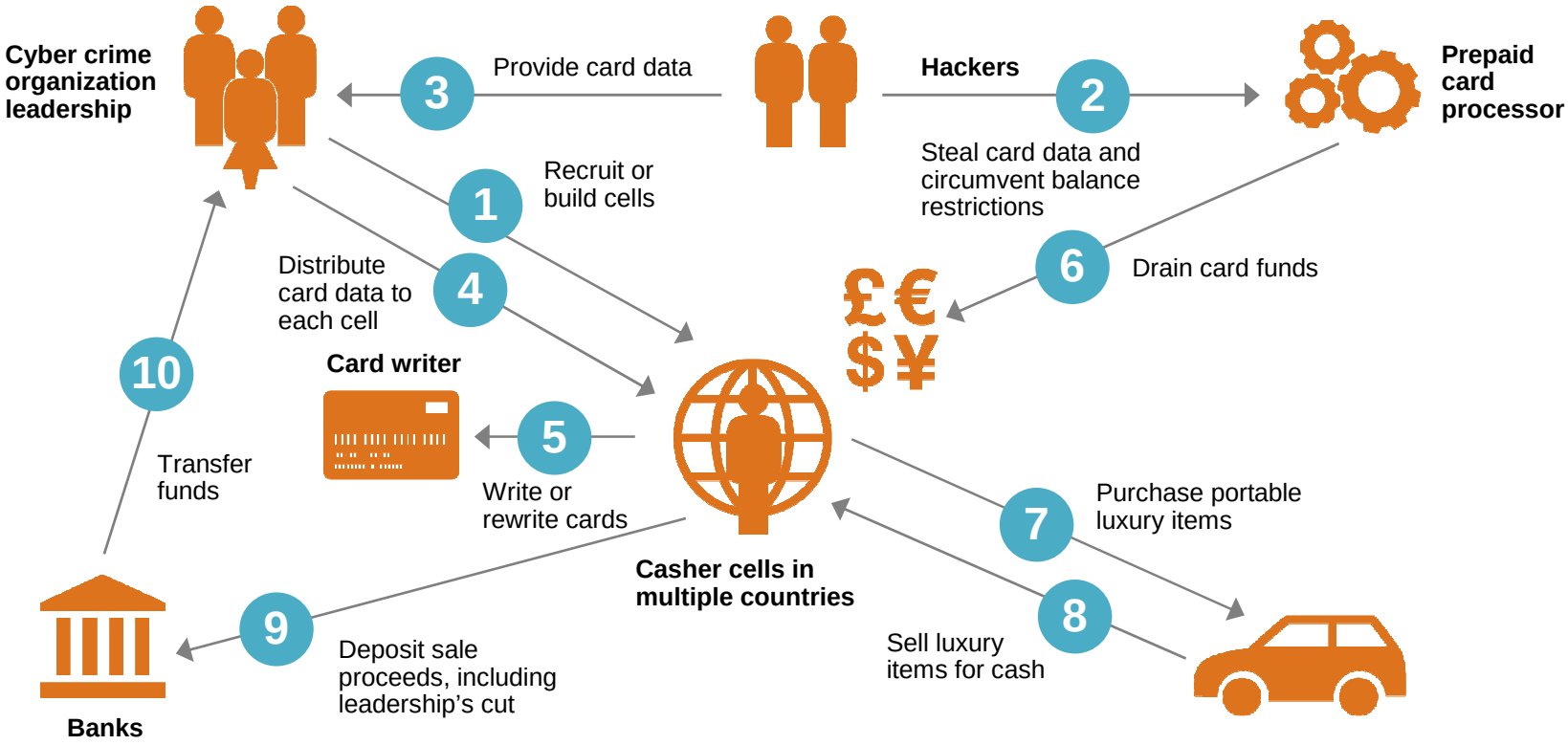
1 2013 Norton Report
2 ACFE
3 2013 Harris Interactive
4 2013 Norton Report
5 Reuters
6 2012 Edleman Survey

All amounts are in US dollars.

IBM

Schemes are increasingly complex, often involving networks of organized activity

Anatomy of a complex fraud scheme



Proactively addressing this can translate into opportunity

Operational effectiveness

IBM client IBC reduced the time to detect a $1 million fraud ring by more than 99 percent from years to days[1]

- **Loss avoidance**
- **Reduce false positives**
- **Focus investigations on high-risk cases to improve efficiency**

Improved customer engagement

IBM client Santam delivered a 70 times faster settlement of legitimate claims[2]

- **Deliver an optimal experience to legitimate customers**
- **Protect customer data**
- **Deter suspicious transactions with confidence**

Brand value

Reputation declines an average of $332 million as a result of an IT breach of customer data[1]

- **Protect your brand reputation**
- **Engender trusted client relationships**
- **Support regulatory compliance obligations**

1 Ponemon Institute, *Reputation Impact of a Data Breach: U.S. Study of Executives & Managers*, November 2011.

All amounts are in US dollars.

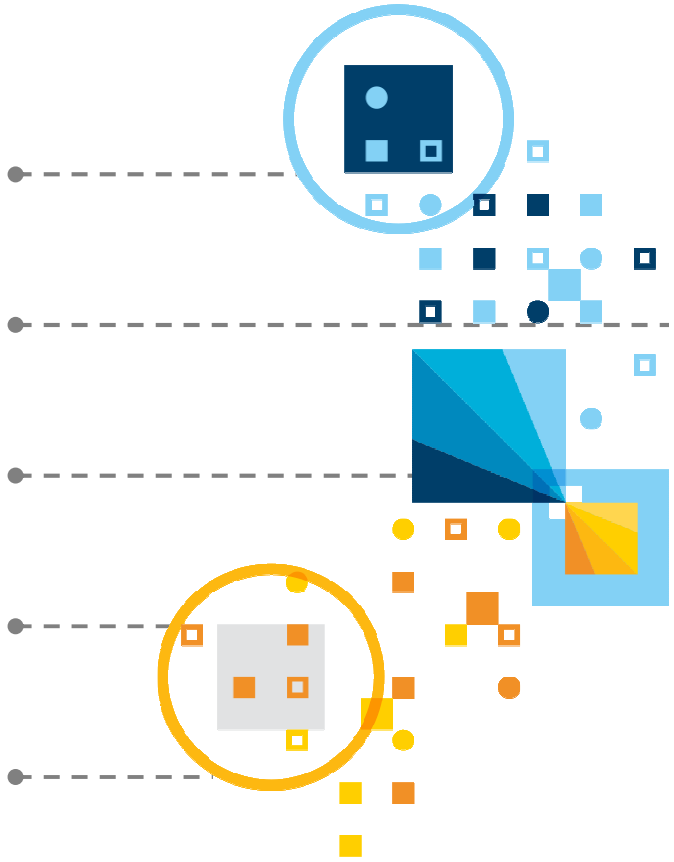
Organizations continue to face challenges in capturing this opportunity

Internally, point solutions and corporate silo mentality contribute to increased risk of fraud and financial crimes:

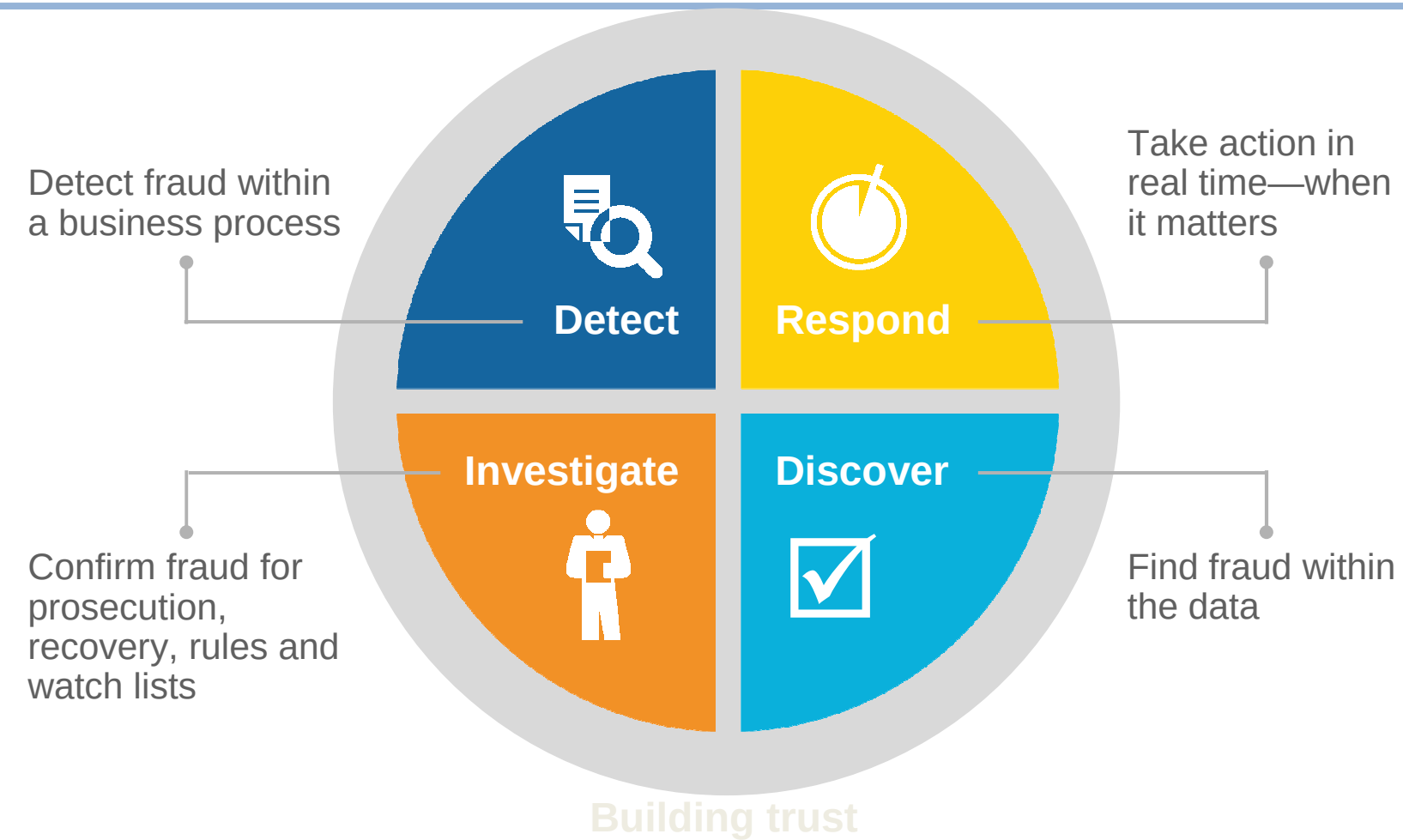
- Analysts and investigators
- Claims
- Analytics
- Legal
- Risk
- Underwriting
- Management

The challenges:

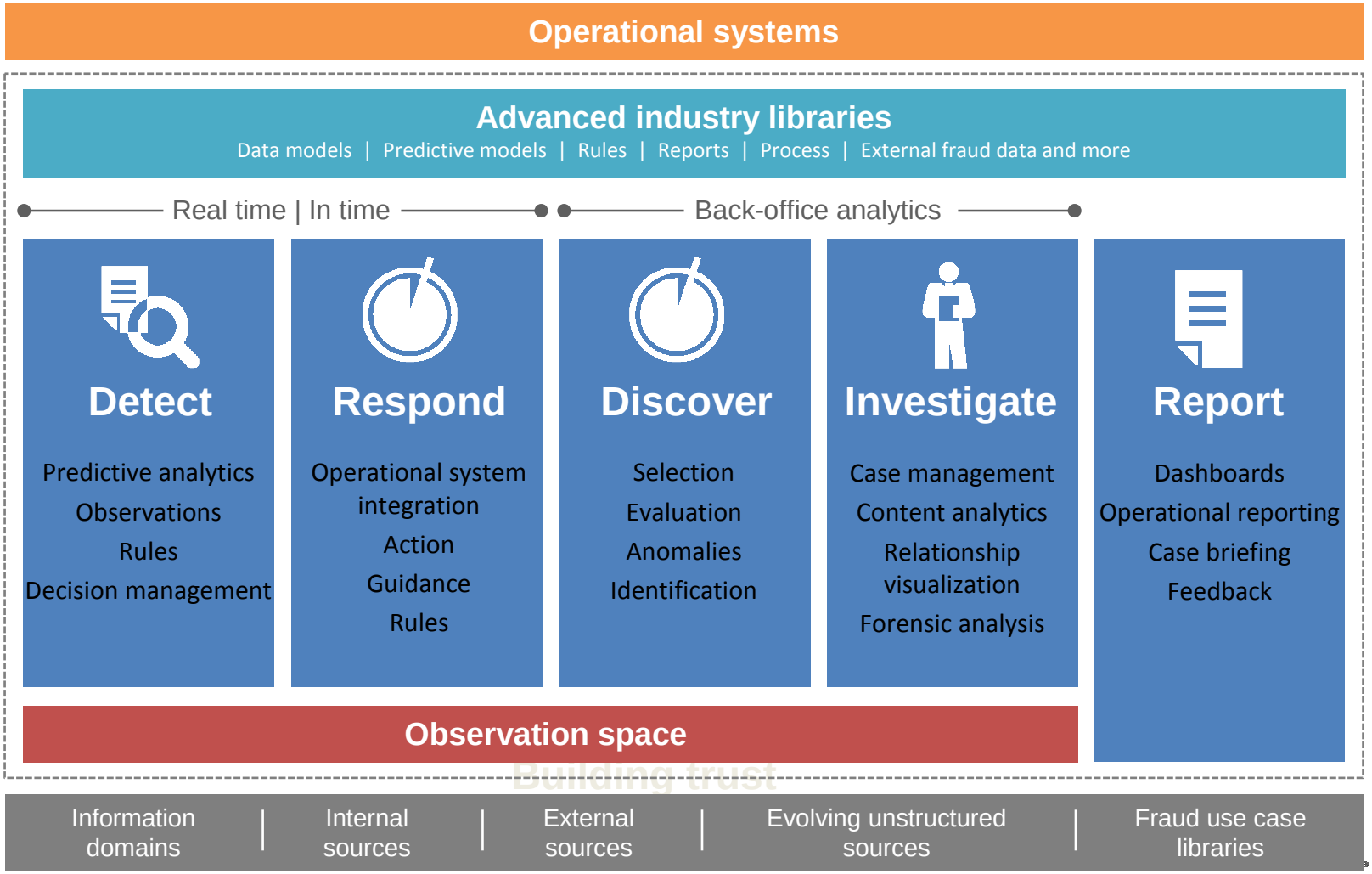
- Prolonged action
- High IT costs
- Transparency and compliance reporting are difficult
- Fraudsters slip in through the gaps
- Difficult to act nimbly to counter the threats



Counter-Fraud Management addresses each phase of an enterprise fraud approach



Counter-Fraud Management offers distinctive and robust capabilities



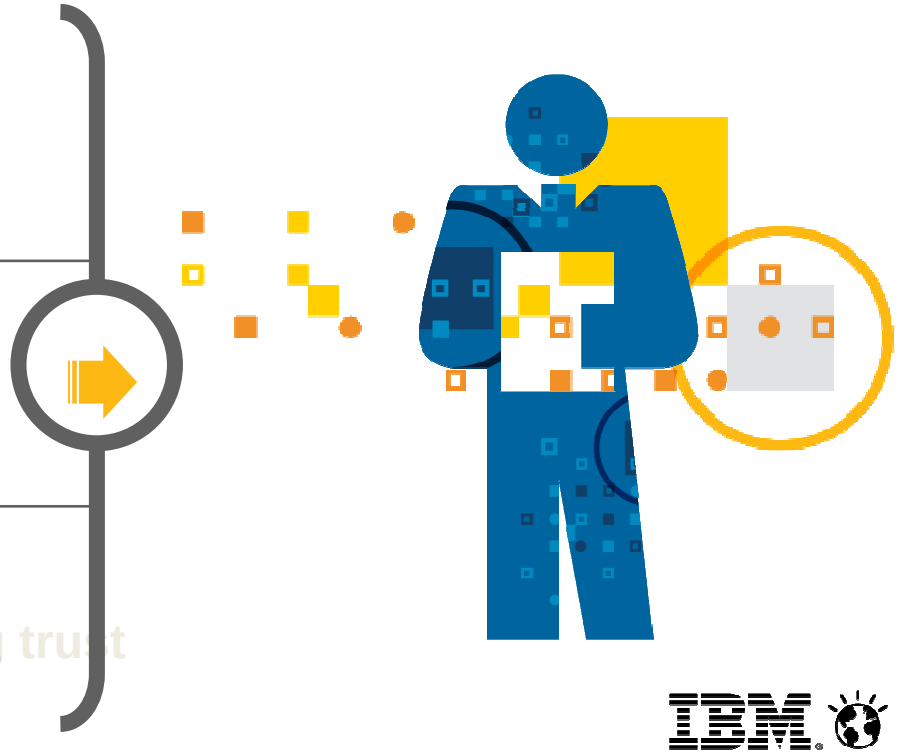
Why Counter- Fraud Management?

For smart organizations, fraud is not treated as a point solution or as a step in the process. It is more than a “score.” It starts before intake. It is seen as preventable, predictable and provable and is managed pervasively across the process lifecycle.

Collaboration
Drives transparency across users and provides guidance and alerts that improve smart decisions

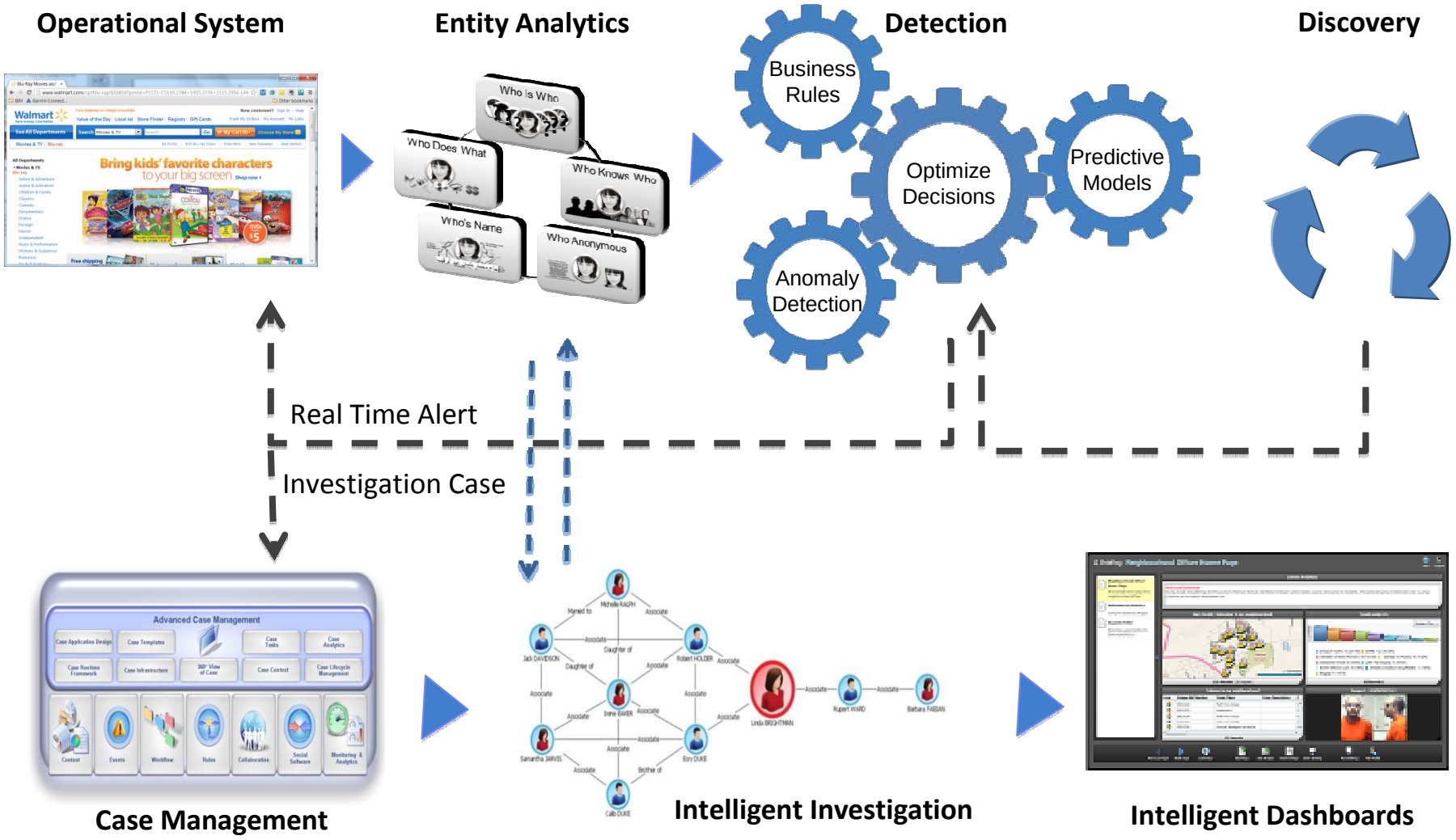
Multilayered
Considers a broad set of attributes, such as identity, relationships, behaviors, patterns, anomalies and visualization

Smart
Exhibits “smart” tendencies: it predicts, detects, discovers, manages, learns and more

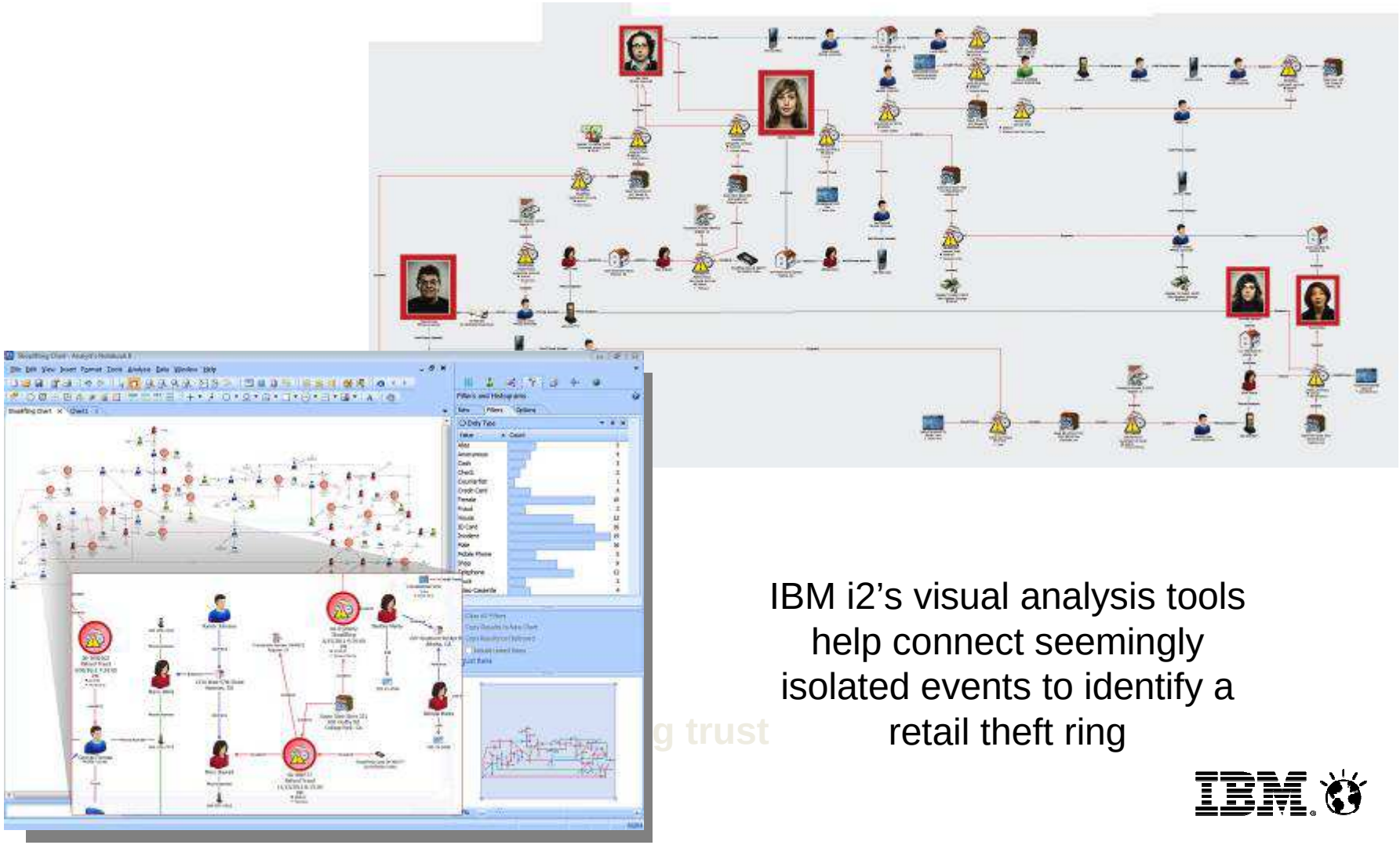


IBM

Detection, prevention, discovery, investigation



Intelligent Investigation, a Retail fraud analysis visualization



IBM i2's visual analysis tools help connect seemingly isolated events to identify a retail theft ring

IBM

Reduce losses due to theft by at least 5% to 10% (0.08% to 0.15% of annual sales overall) with IBM i2 due to faster detection, improved productivity, higher prosecution rates, and increased recoveries

Performance Improvement and Benefits

Benefit	Rationale
Faster detection	Shut down criminal activity sooner due to integrated data, auto alerts, and improved overall case review and investigation times
Increase case capacity	Open (and close) more cases per investigator due to ability to tie multiple related cases into one and more efficiently manage case materials (ie, with IBM i2workflow)
Improve case success / prosecution rate	Improve identification and prosecution of criminals due to more complete body of relevant data, more powerful analytics, and identification use of LE recognized language and reporting
Increase recoveries per case	Increase recoveries due prosecution of larger networks with more assets for seizure detected with more complete views of linked criminal activities

Key Estimates and Assumptions

Net Annual Bottom-line Benefit Potential =
$70 million to $140 million

- Annual sales = $97 billion (est.)
- Annual losses due to theft and fraud = 1.5% sales ($1.4 billion)
- Estimated annual reduction in losses due to i2 FIA = 5% to 10% ($70 to $140 million)

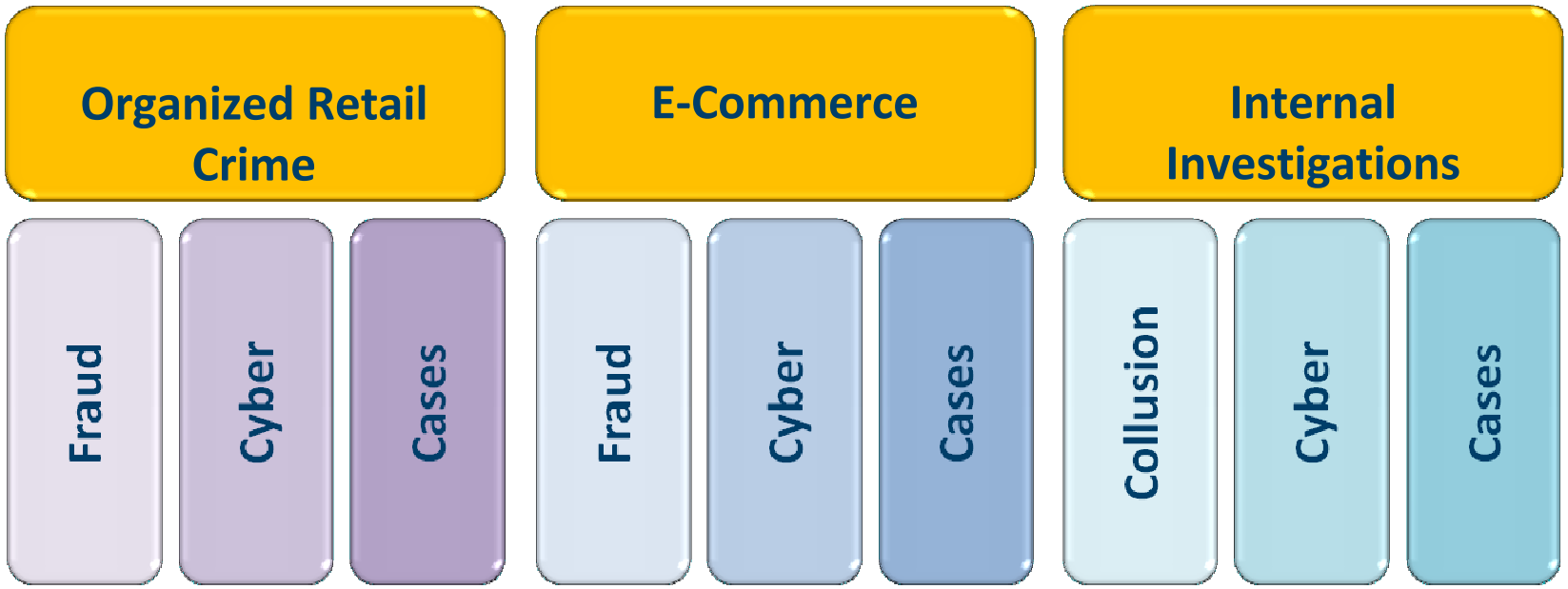
- Note: Estimated one-time reduction in excess inventory (because theft increases safety stock) = $40 to $100 million

Each case may be a single piece of the puzzle…

Threats are often connected…
Threat investigations generally aren't

IBM

Internal organizational lines create barriers



Shared intelligence breaks down barriers

Analysts

Investigators

Executives

Shared intelligence repository

Organized Retail Crime			E-Commerce			Internal Investigations		
Fraud	Cyber	Cases	Fraud	Cyber	Cases	Collusion	Cyber	Cases

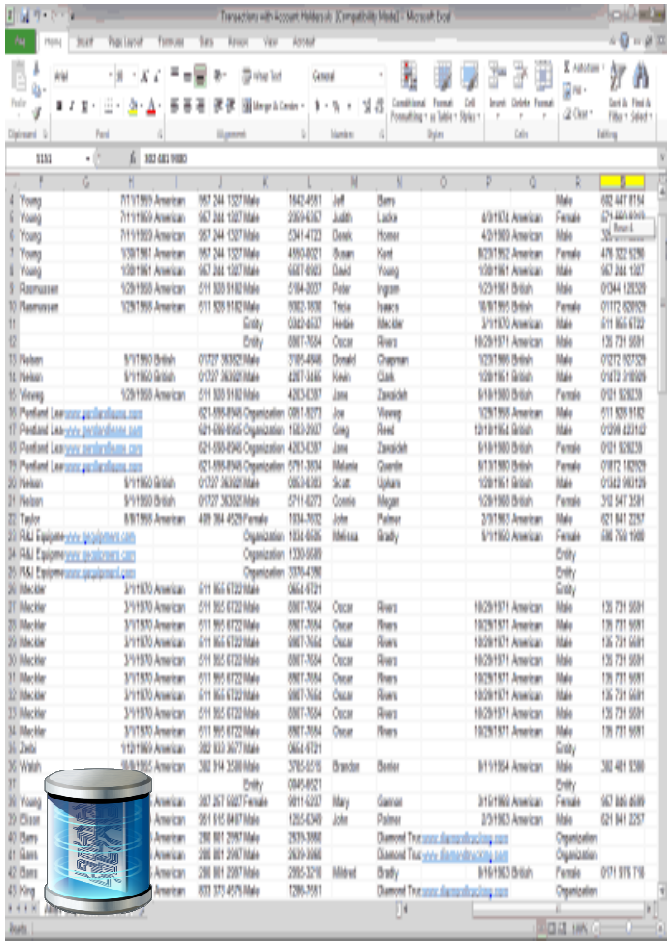
IBM

Turn information into intelligence to drive action

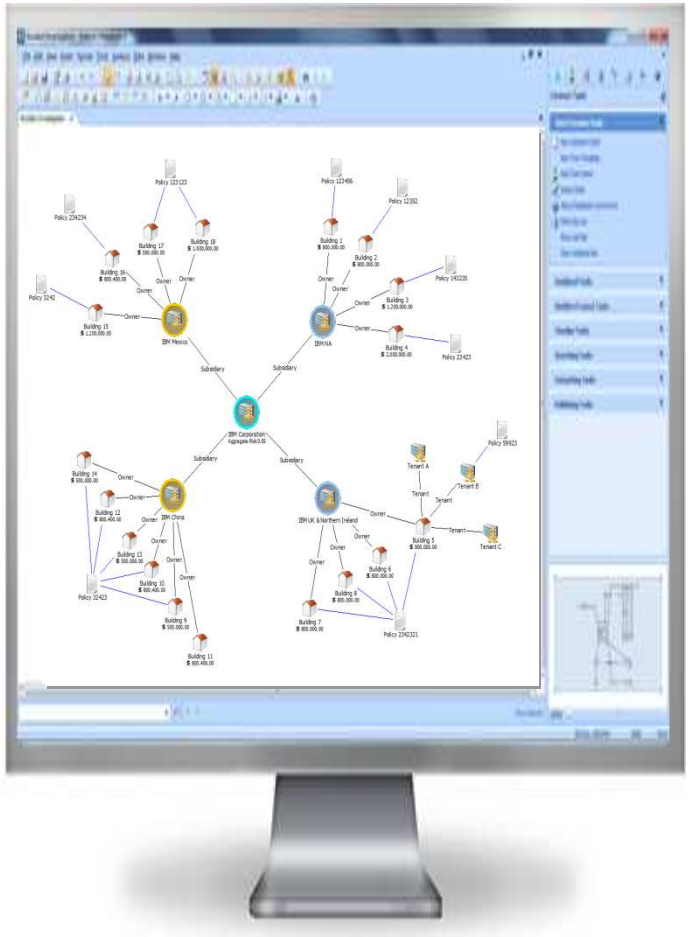
Channels

- Online
- Service Centers
- Email / Chat
- Third Party Data
- Mobile

Data



Intelligence



Investigators will be able to manage more cases at a time, and process cases more quickly, by integrating data, speeding collection and reporting, and accelerating each stage of the review process

What We've Heard:

"Takes 'quite a while' (eg, several hours) to search multiple different data systems"

"Today each investigator determines when 'enough' information has been collected"

Technology Barriers:

- Fragmented transactional and security data sources / no master database
- Limited data search and analysis tools for investigators

Enabling Capabilities:

- Automate collection of data from specific data sources
- Investigators create own ad hoc federated searches across multiple data sources
- Predictive fraud analytics, entity resolution, link analysis, transactional analysis and geospatial analysis
- Complex algorithms for Social Network Analysis to better apply focus and resources
- Heat matrices, histograms, and filtering to quickly identify hidden relationships in the data

Benefit / Improvement Opportunities:

- Increase case capacity without adding resources due to ability to tie together multiple related cases into one and Improve overall case review and investigation times
- Reduce case cycle time due to faster turn around of investigation data improving team speed and efficiency
- Lower cost due to better data availability and more efficient collaboration (fewer resources working the same case)
- Better data accuracy and completeness without manual manipulation or multiple query attempts for the same information

IBM

[Major Retailer] will realize higher recoveries and an improved success / prosecution rate with a more complete view of criminal networks and patterns (past and present)

What We've Heard:

"No analytics today on multiple investigative requests or for commonalities between current and past patterns"

"Today we can't detect identity theft schemes…the common denominators are hidden to us"

Technology Barriers:

- Fragmented transactional and security data sources / no master database
- Limited data search and analysis tools for investigators

Enabling Capabilities:

- Enterprise intelligence repository for collaboration
- Rapid, powerful Information Analytics
- Investigator control of data gathering and report generation
- Alerting functionality makes team members aware of shared interest in an individual or group
- Web portal gives "Google" like search access to external team members
- Detailed security options to protect data distribution
- Complete evidentiary material governance

Benefit / Improvement Opportunities:

- Increase recoveries per case due to more complete view of linked criminal activities resulting in prosecution of larger networks with more assets for seizure
- Improve success rate due to inclusion of more complete body of relevant data, more powerful analytics, and responsiveness of law enforcement (LE)
  - Fresher data, use of LE terms/formats, and larger fraud networks means a better chance of pursuit and prosecution of the criminals
  - Improved collaboration and automatic alerts drive deeper insights leading to more successful cases

IBM

Thank you!

Building trust

IBM