Un approccio omnicomprensivo per la prevenzione delle frodi

Giovanni Todaro, IBM
Laura Passa, IBM

Organizations lose an estimated 7 percent of annual revenues to fraud

$994 billion in the US alone

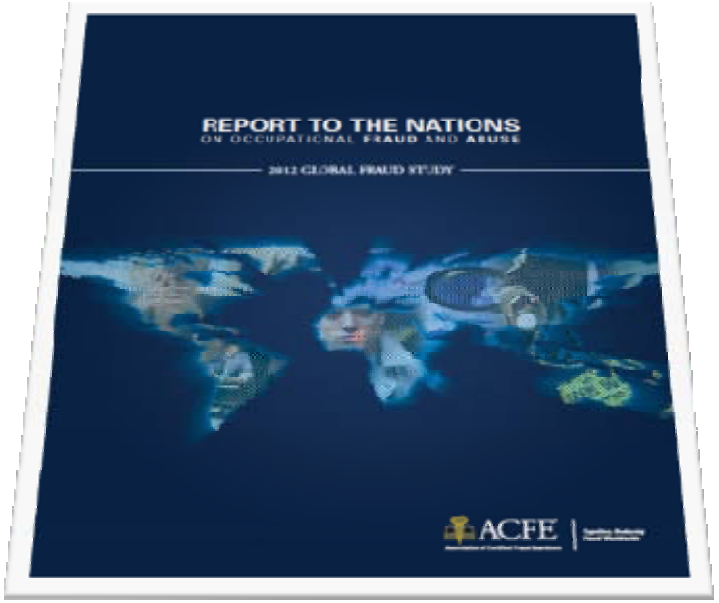
- **Economic downturns lead to greater fraud and abuse**

  Individuals and businesses seek new ways to create revenues, not necessarily legal ones
- **Market conditions pressuring our customers bottom line**

  Need to find additional ways to improve results
- **Fraud is getting increasingly complex**

  Fraudsters continue to increase their sophistication
- **Advances in analytics and big data make finding and preventing fraud more effective**

  We can do now what we previously couldn't.



- Occupational Fraud is estimated to cost organizations $3.4T annually.
- Survey participants estimated that the typical organization loses 5% of its revenues to occupational fraud each year.
- 20% of the cases were greater than $1M.
- The frauds reported to us lasted a median of 18 months before being detected.

Converging forces are creating the “perfect storm” for heightened focus around fraud and financial crimes

Schemes are increasing in complexity and frequency

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

Economic and societal costs of fraud have escalated

Intensifying regulatory enforcement and operational losses apply significant pressure on profitability

Customer expectations have intensified

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

12 per second

Cyber crime victims

80%

Originate in organized activity

The 2013 Norton Report

$4.7 trillion

Global cost of fraud today

$1.92 billion

Fine in money laundering case

Reuters

71%

Customers who will switch banks due to fraud

2013 Interactive Harris

46%

Customers leaving/avoiding companies with a security breach

2012 Edleman survey

We are in an era of continuous breaches

Attackers are relentless, victims are targeted, and the damage toll is rising

Operational Sophistication

IBM X-Force® declared **Year of the Security Breach**

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

Relentless Use of Multiple Methods

500,000,000+ records were leaked, while the future shows no sign of change

2011 2012 2013

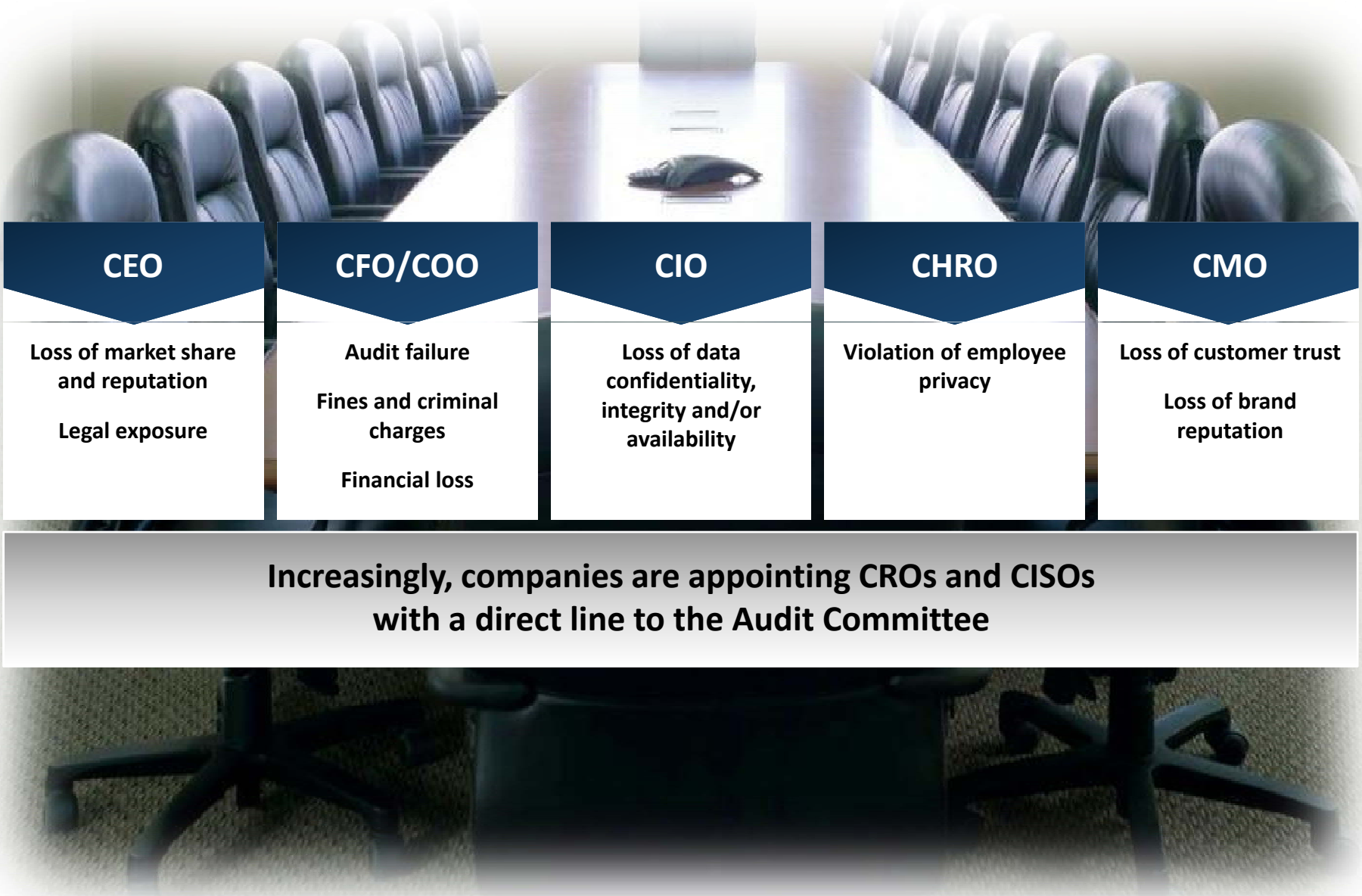
Attack types

SQL injection | Spear phishing | DDoS | Third-party software | Physical access | Malware | XSS | Watering hole | Undisclosed

Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2014

Note: Size of circle estimates relative impact of incident in terms of cost to business.

Countering Fraud and Financial Crimes is a Board Room issue



CEO	CFO/COO	CIO	CHRO	CMO
Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy	Loss of customer trust Loss of brand reputation

Increasingly, companies are appointing CROs and CISOs with a direct line to the Audit Committee

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

Four truths about advanced threat protection

Despite increasing challenges, organizations can protect themselves by adopting the right strategy

1 Prevention is mandatory

Traditional methods of prevention have often failed, leaving many to believe detection is the only way forward. This is a dangerous proposition.

2 Security Intelligence is the underpinning

Specialized knowledge in one domain is not enough. It takes enterprise-wide visibility and maximum use of data to stop today's threats.

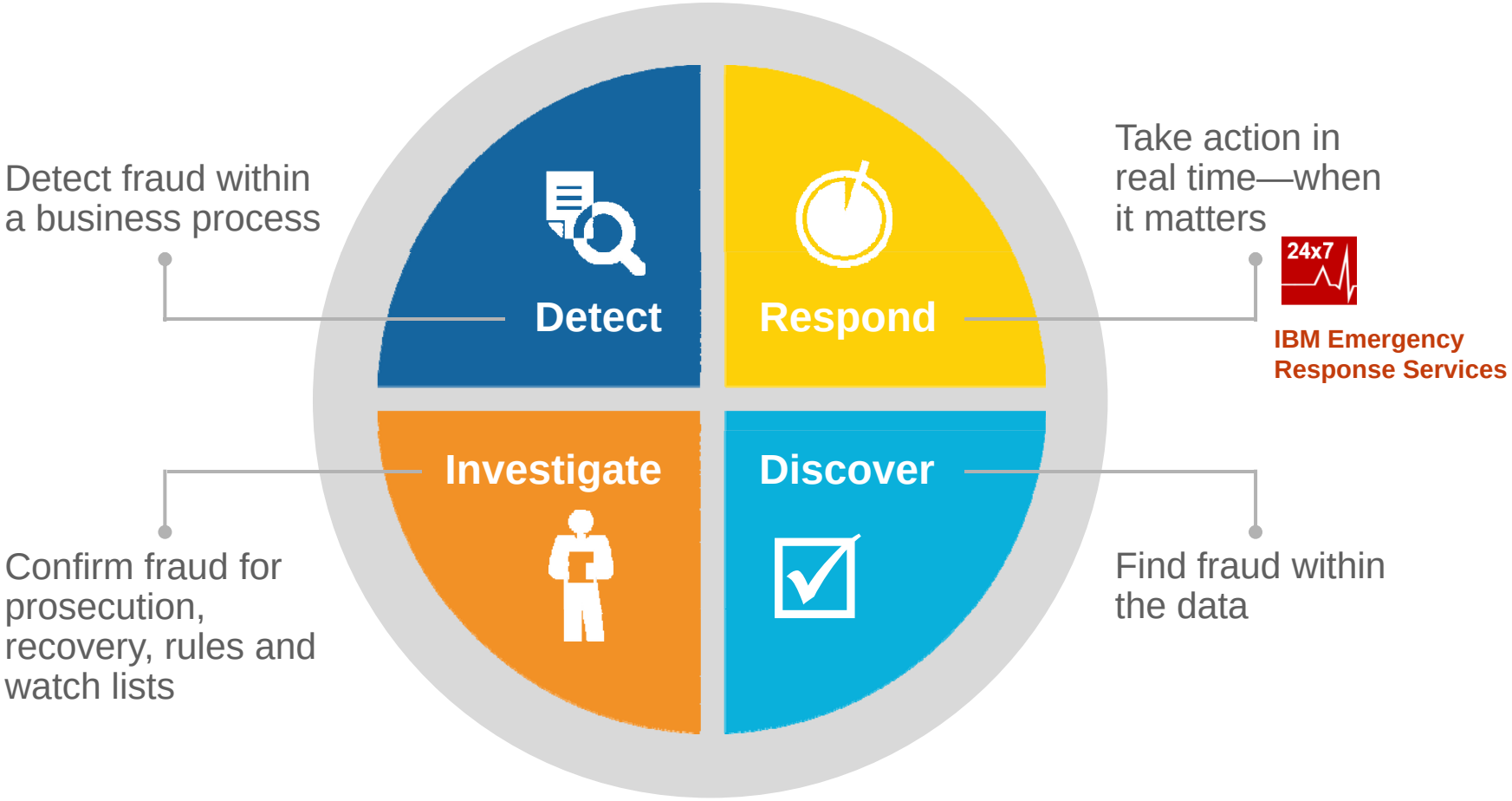
3 Integration enables protection

The best defense is relentless improvement. Technologies must seamlessly integrate with processes and people across the entire lifecycle of attacks.

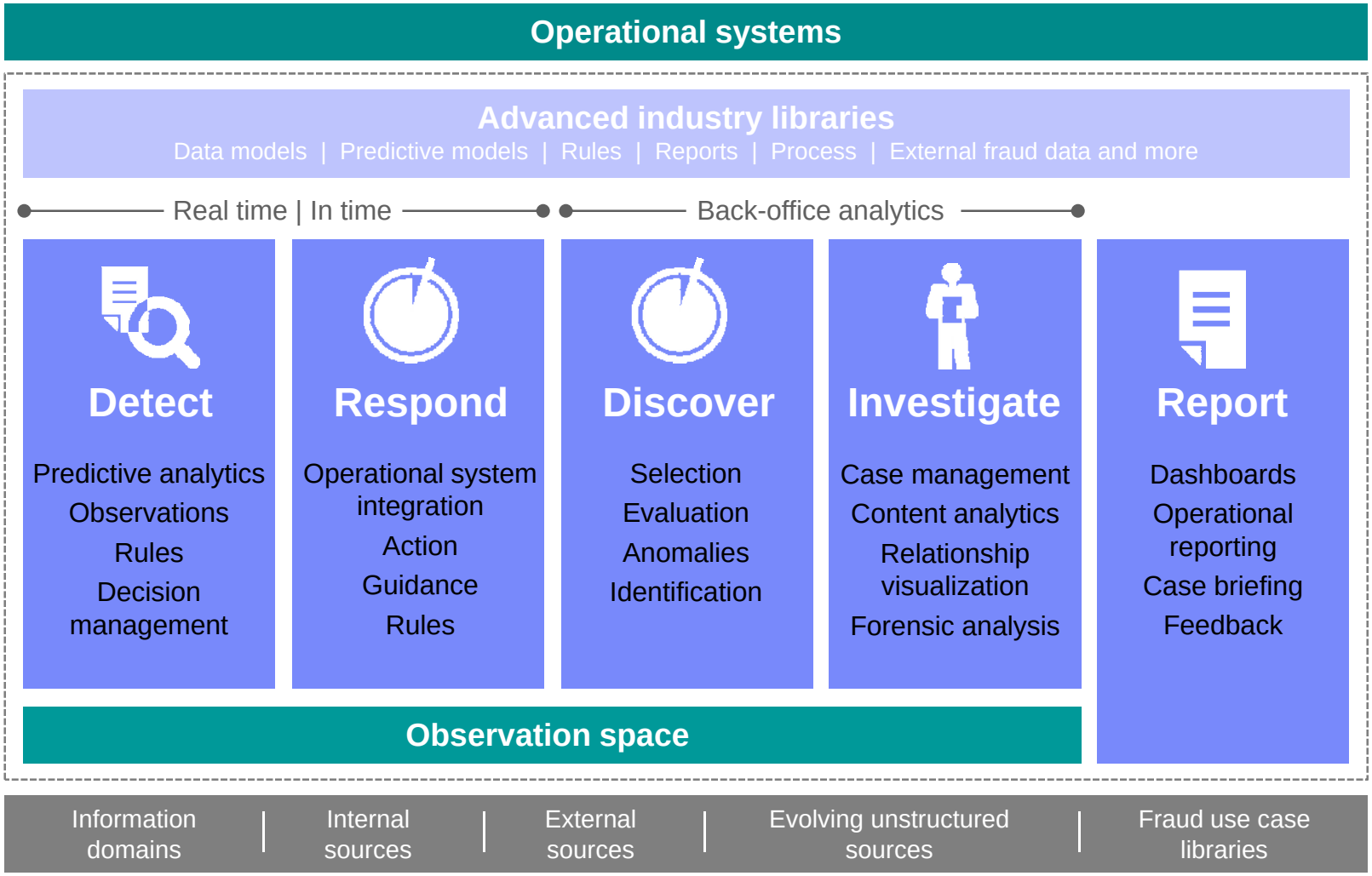
4 Openness must be embraced

Security teams need the ability to share context and invoke actions between communities of interest and numerous new and existing security investments.

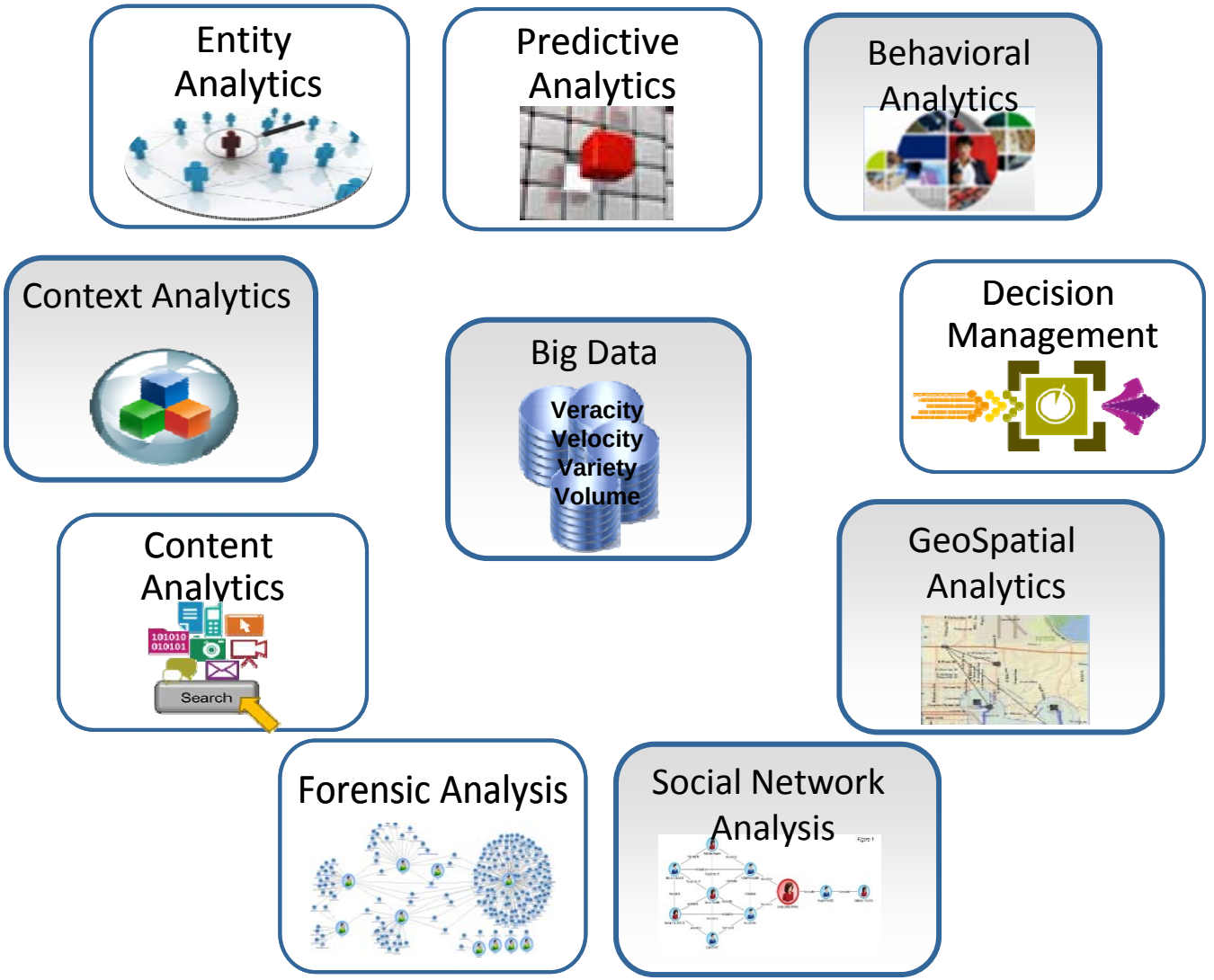
IBM Counter-Fraud Management addresses each phase of an enterprise fraud approach



IBM Counter-Fraud Management offers distinctive and robust capabilities



IBM Counter-Fraud Management employs multi-layered analytical techniques



Grupo Bancolombia uses data mining to identify potentially fraudulent transactions

40% increase
in identifying suspicious transactions

200% increase
in reporting capabilities

80% increase
in analysis productivity

Business Challenge: To adhere to stricter governmental reporting requirements, Grupo Bancolombia needed to analyze millions of daily transactions to identify current and potential fraud.

The Solution: The bank deployed predictive data-modeling software that helped it more easily and quickly detect transactions that were part of potential money-laundering operations. By detecting and analyzing expected and typical patterns of over 1.3 million transactions per day, the solution prevents, detects and reports potentially fraudulent banking activities that may stem from criminals and terrorists.

"With the data mining system, we generated productivity savings of nearly 80 percent."

— Francisco Ruiz, Head of Compliance, Bancolombia

Bancolombia

Case Study 1: Improve Fraud Operations through enhanced Detection

Business Challenge

•The largest fraud loss realized by client bank is a result of Deposit fraud.
•Current system generates many alerts that turn out to be false positives (approximately 99%)
•In addition, it does not evaluate all transactions and as such, does miss potential fraudulent transactions

Project Overview

•6 Months POC project leveraging IBM's Counter Financial Crimes Management solution, applied against "live" data, demonstrated clear and compelling business value to the client

Solution Overview

- **Business Solution:**
  - Built deposit fraud model, rules and entity-centric resumes using historical customer and watch list data
  - Provided "Insights" for every alerted transaction
  - Identification of low risk & high risk cases to improve prioritization of cases
  - Integrated results from multiple scoring streams into a single recommendation

- **Technical Solution:**
  - Data ingested from multiple sources (client provided and external watch lists) into the analytics environment
  - Insights were developed using data mining and statistical analytics, entity analytics and business rules
  - Provide a prioritized list of alerts ranked from highest to lowest scores, with key fraud indicators for use in investigation

Business Results

- Reduced false positive rates by **9-15%**
- Increased the potential of finding fraud by **130%**
- Solution delivered **2.3x greater efficiency** in finding "fraud" than incumbent, with an **increased fraud value of $9.4 million** on an annualized basis
- Better quality detection results lead directly to increased investigator efficiency

Summary

1. “If you cannot see the full picture you cannot respond”
2. “Fraud is a board discussion and you need to have an Enterprise Fraud Management Strategy”
   - *Prevention is mandatory*
   - *Security Intelligence*
   - *Integration enables protection*
   - *Openess must be embraced*
3. “IBM Counter-Fraud Management addresses each phase of an enterprise fraud approach”
   - Detect
   - Respond
   - Discover
   - Investigate
4. Next Step: Business Value Assessment