IBM `Information Management` software

IBM Real-Time Collaborative Criminal Investigation and Analysis: Identify criminal and terrorist threats

Highlights

- *Implement an integrated end-to-end solution across dispatch, investigation, case management, records and staffing*

- *Address growing public pressure to deliver more secure protection services to counter terrorism*

- *Provide police officers with a solution that supports and empowers them to make better real-time decisions during criminal investigations*

- *Help manage risk by detecting and mitigating threats and following up on leads for persons or networks of interest*

- *Protect privacy of suspect and offender information with internal and external entities*

- *Integrate intelligence sharing with Department of Homeland Security and public safety agencies*

- *Build on existing investments to optimize investment in skills and infrastructure*

- *Receive perpetual and preemptive alerting for persons of interest (POI) and their relationships*

The high-stakes world of law enforcement

Some of the greatest strengths of a free society are its openness and interconnectedness—but these qualities also can be some of its greatest vulnerabilities. Given these issues, how can law enforcement agencies protect diverse populations across large geographic areas? How can they balance the need to protect and serve with the need for personal privacy and freedom?

In addition to these external forces, internal pressures are common across law enforcement groups: shrinking budgets, inadequate legacy systems, increasing demands to detect and reduce internal and external threats, and the expectation that agencies find ways to do more with less. With these

pressures, law enforcement agencies are facing strategic issues that require major changes in the way they conduct business. Law enforcement organizations must innovate and develop new approaches to deliver security and protection more quickly, effectively, responsively and efficiently and provide better service to citizens.

A fresh approach to threat management

Threats to safety and security can manifest themselves in many ways. For example, suppose a terror suspect commits a minor infraction and is stopped by police. The suspect may be operating across multiple jurisdictions, but the officer on patrol would have no way to know that the recipient of the speeding ticket is a wanted terrorist. The local police department is not even likely to be aware that the suspect was ticketed in another jurisdiction the previous week.

"NYPD's innovative policing strategies depend on our ability to gather, share and act on information. IBM—its people, partners and technology—have helped us redefine how information can be used to fight crime."

—*James Onalfo, Chief Architect and CIO, New York Police Department*

The core problem is that most law enforcement agencies have no way to resolve multiple identities used by terrorists and criminals, or to track relationships and conspiracies among them. Adding to the complexity, when personal information is obtained from outside the department, the need to protect the privacy of the individuals under investigation further intensifies the challenge.

Today's law enforcement challenges mandate a fresh approach to managing threat information based on a variety of factors. These factors include exponential growth in threat types and frequency, growth in the number of asymmetrical threats, an explosion in the complexity of threat identification, increased frequency of interaction with terror suspects, decreased transparency, mounting regulatory pressures and intensifying budget pressures.

Current approaches to threat reduction have become obsolete. In many agencies, information is compartmentalized, and this lack of full integration can obscure visibility. Law enforcement officials have a limited ability to address complex threats because they need to know the right questions to ask, yet they frequently lack complete information. Threats are often identified only after the fact, and false positives and false negatives occur regularly. In addition, information is often out of context and officials lack appropriate decision support and guidance once a threat is identified.

The IBM solution for rapid, effective case management
The IBM® Real-Time Collaborative Criminal Investigation and Analysis solution provides an end-to-end approach through a platform for differentiated investigative analysis tailored to individual suspects. It also enables organizations to share information in a form that protects the privacy of their suspects.

Key features include:

- *Recognition of multicultural names and multiple name variations* such as Kate, Cait, Catherine, Katherine and Kat; the platform also can handle variations in name order, multiple titles, name variants, multiple prefixes and phonetic transpositions of nicknames
- *Recognition of identities that provides the ability to identify people and organizations, even when they are deliberately attempting to disguise themselves*
- *Recognition of relationships between a suspect and other individuals or organizations*

> *IBM provides law enforcement agencies the ability to share identity and relationship information without disclosing the identity of the person to whom the information relates.*

Risk assessment

For each case, law enforcement agencies must determine whether each suspect should be investigated and pursued. Once the agency establishes the degree of risk associated with the case, it can determine which resources should be applied to each case.

Threat and fraud intelligence solutions from IBM help law enforcement

agencies perform these tasks by enabling them to:

- *Provide full attribution with a complete history of a suspect or criminal*
- *Never dispose of, merge or purge data about individual suspects*
- *Receive real-time, self-correcting updates that help create and maintain a current, more accurate view of each suspect*

- *Achieve relationship insight in cases of multiple degrees of separation (for example, Suspect A knows Suspect B, and Suspect B knows Suspect C; therefore, the three are related by two degrees of separation)*
- *Segment suspects to help detect individuals of higher risk in order to focus appropriate attention and resources on these suspects*

Privacy protection

Information about suspects is needed to successfully follow up on leads and process cases. Since the suspect usually provides the information, there is not a privacy issue. However, difficulty arises when elements of information are combined in ways that reveal more about a person's private life than intended.

Each country takes a different approach to privacy, and many have legislated privacy into their law enforcement systems. Unfortunately, privacy protection has become an inhibitor to good police service in many cases. However, citizens would be much more willing to allow privacy information to be shared if asked, and they would benefit by providing consent.

IBM provides law enforcement agencies the ability to share identity and relationship information with third parties without disclosing the identity of the person to whom the information relates. This capability supports the police services delivery model, which is oriented around integrated service, citizen consent and choice.

Intelligence fusion for Homeland Security

The shocking realization that terrorists can strike within United States borders has affected citizens' lives directly and elevated the need for vigilance. To facilitate intelligence gathering, the President of the United States and the U.S. Congress have mandated an enhanced information sharing environment across the federal government, as well as across many state, local and tribal entities.

The Department of Homeland Security has established guidelines for operating these "fusion centers" and sharing intelligence and information at the local, state and federal levels. Using the IBM Real-Time Collaborative Criminal Investigation and Analysis solution, organizations can:

- *Exchange information among agencies*
- *Automate the resolution of identities in real time*
- *Discover and analyze relationships within gangs or terror networks*
- *Identify new patterns and trends*
- *Receive real-time alerts based on newly linked identity information*
- *Recognize multiple cultural variations of name data*

Proven methods, tools and techniques

IBM has invested significant resources in the Real-Time Collaborative Criminal Investigation and Analysis solution. The solution brings together a range of methods, tools and techniques specifically designed to enhance the implementation of integrated case and risk management solutions within law enforcement organizations. This criminal intelligence solution features technology for handling cases, risk management and privacy, and fusion centers tailored to individual law enforcement agency requirements.

IBM offers a dedicated team of subject matter experts, solution developers and industry consultants that are focused on law enforcement and intelligence.

A solid foundation built on world-class technologies from IBM

IBM is one of the world's largest providers of solutions to intelligence and law enforcement organizations. IBM offers a dedicated team of subject matter experts, solution developers and industry consultants that are focused on law enforcement and intelligence. IBM has invested in a portfolio of solutions for the threat and intelligence industry and provides a leadership role in helping organizations take advantage of global best practices in safety programs.

The IBM Real-Time Collaborative Criminal Investigation and Analysis solution is built upon several specific functions:

- ***IBM Global Name Recognition:*** *Recognizes names across multiple cultural variations*
- ***IBM Identity Resolution:*** *Identifies and organizes information on individuals so law enforcement officials know the true identity of the individual*
- ***IBM Relationship Resolution:*** *Identifies individuals who know one another across multiple degrees of separation*
- ***IBM Anonymous Resolution:*** *Allows multiple organizations to share identity and relationship data anonymously so individual identities are never disclosed*

For more information

To learn more about IBM Threat and Fraud Intelligence solutions and the IBM Real-Time Collaborative Criminal Investigation and Analysis solution, please contact your IBM sales representative, call toll-free (U.S.) 1-866-382-9774 or visit **ibm.com**/software/data/ips/solutions/tfi

IBM

TAKE BACK CONTROL WITH **Information Management**