Enterprise Security – Cyber Security APAC Forum

David Louey Gung
Director Justice & Public Safety APAC
Agenda

- Police Security Requirements
- Major Challenges for Law Enforcement Agencies
- Oracle Enterprise Security Solutions
- Innovative secure solutions for Disaster Management – Case Studies
Victoria Police IT infrastructure - Security Requirements

- In 1993 the current HRMS and Operational Police RMS were implemented on the Mainframe.

- Very little technology existed in the 380+ police stations

- Uniformed police developed their own local applications and (standalone) LANs at 20 stations.

- 1999 IT infrastructure rolled out
  - Shared Govt WAN – VPN
  - Standard LANs, servers & desktops installed
  - Username/Password access validated from HRMS
  - Password resets highest no. H/desk Calls (single sign-on)

- 2001 (ROI) - Oracle Financials & Website implemented
  - Security Report showed ~80K attempted breaches/month
  - Penetration test commissioned → security weakness
Victoria Police Applications - Security Requirements

- 2004 Centralized Management of Apps (20 to >400)
  - Few complied with Security Policy & Privacy Law

- Inappropriate use of police information
  - Police Officers who breached security and privacy policies disciplined / heavy fines

- Reason for LEAP/RMS access implemented

- All LEAP/RMS changes audited (separate to DB audit records)

- LEAP/RMS Audit records analyzed regularly by police auditors to determine cases of appropriate use.
2004 Crime Dept evaluated Enterprise Investigative Case Management solutions for intelligence gathering to address major crime:

- Security considerations the No. 1 requirement.
- Restrict Case Access to Investigating Team
- Team Lead to nominate team members’ access
- Senior team members only to access certain info
- Hide info. from Systems Administrator & DBA
- Enabled Internal Investigations to migrate across
Major Challenges for Law Enforcement Agencies

• Major Challenges are:
  • Organised Crime
  • Terrorist Activity
  • Cyber Crime

• Transnational nature, create global issues that become domestic issues

• Oracle has dedicated resources with domain expertise and technology solutions to assist Law Enforcement agencies address these challenges.
The Challenges We’re Hearing

**Fragmented Police and Intelligence Information**

“How can we create a trusted environment for the sharing of critical information across departments and jurisdictions?”

Clues and evidence related to criminal or terrorist activity are often spread across disconnected databases and paper files stored in thousands of law enforcement databases.

Gartner, Facing Information-Sharing Challenges Among Law Enforcement Agencies

**Inability to Analyze and Act on Crime Information**

“How can we identify trends and patterns to anticipate and prevent incidents?”

Organizations should designate a group of individuals to be responsible for collecting and analyzing crime information and other performance-related data to improve an agency’s understanding of the incidence of crime and how an agency combats it.

Gartner, Take These Four Steps When Adapting Your Organization to the CompStat Model

**Limited Resources**

“How can we reduce crime and combat terrorism with limited resources?”

Police forces are now dealing with crime that would be unrecognizable to police officers of a generation ago and must do so with a rapidly shrinking resource base.
Oracle – > 30 Years of Security Leadership

1977
- Trusted Oracle7 MLS DB
- Government customer (CIA – Project Oracle)

2009
- Audit Vault
- Database Vault
- Content DB, Records DB
- Secure Enterprise Search
- Thor & Octet String (IdM Acquisitions)
- Phaos, Oblix, (IdM Acquisitions)
- Database CC Security Eval #18 (10g R1)
- Transparent Data Encryption
- VPD Column Sec Policies
- Fine Grained Auditing (9i)
- 1st Database Common Criteria (EAL4)
- Oracle Label Security (2000 8.1.7)
- Virtual Private Database (1998)
- Enterprise User Security (8i)
- Database Encryption API
- Kerberos Support (8i)
- Support for PKI
- Radius Authentication
- Network Encryption (Oracle7)
- Oracle Advanced Security introduced
- First Orange Book B1 evaluation (1993)
- Trusted Oracle7 MLS DB
- Government customer (CIA – Project Oracle)
Oracle in Justice and Public Safety

Did You Know?

8 of the top 10 largest Law Enforcement Agencies in the U.S. And Canada use Oracle Technology and/or Applications

15 of the 25 European Union Member Nations run Oracle Applications

9 Asia Pacific Country Governments run Oracle Applications

The U.S. and Canadian Intelligence Communities and Departments of Justice run Oracle
## Oracle’s Justice and Public Safety

### 21st Century Next-Generation Justice & Public Safety Information Systems

#### Integrated Justice Community Collaboration
- Citizen Portals
- Community Outreach
- National, Regional & Local Law Enforcement
- Cross Jurisdictional Law Enforcement
- Cross Jurisdictional Intelligence

#### Overlay Infrastructure for Investigation, Apprehension, Prosecution and Emergency Response
- Analytics & Business Intelligence
- Business Process Management
- Master Data Management
- Unified User Interface
- Data Integration Services

#### Law Enforcement
- Intelligence Gathering and Analysis
- Investigative Case Management
- Evidence Management
- Emergency Preparations & Response

#### Courts
- Litigation Case Management
- Jury & Trial Management
- E-Filing & E-Discovery
- Court Records Management

#### Corrections
- Offender Management
- Prison Records Management
- Community Programs
- Prison Management

#### Border Control
- Surveillance
- People & Cargo Entry & Exit Management
- Customs & Excise
- Immigration and Asylum Management

#### Administration & Enterprise Management
- IT Services (Help Desk, Etc.)
- Human Resources & Workforce Management
- iLearning & Classroom Training
- Facilities Management & Field Service Auto.
- Performance Management & GRC
- Financial Management
- Grants Management
- SCM & Procurement
- Records Management
- Program / Project Management

#### Infrastructure
- Identity Management & Security Services
- Data & Content Management
- Mobility & Location Services
- Service Oriented & Event Driven Architecture
- Highly Available and Scalable App & Info Svcs

**CONFIDENTIAL:** All capabilities and dates are for planning purposes only and may not be used in any contract.
# Investigative Case Management

## Reduces Administrative Time for Front Line Personnel

### Lead Management
- Use as a secure collaboration tool, natively tied to a case
- Route to the right resource for follow-up and view as part of the parent case

### Evidence Management
- Track all forms of Evidence & provide secure visibility to all parts of the organization
- Tie to “hard” assets

### Incident Management
- Capture complete law enforcement information on external events
- Convert to case and spawn requests for service

### Offenses
- Enter and track all crimes that the perpetrators allegedly committed as part of the incident ("assault")

### Locations
- Track specific locations using GPS coordinates or community nicknames ("the old mill")

### Subjects
- Track individuals whose names are unknown, but statistics are known ("john doe")

### Offenders
- Track known perpetrators of criminal offenses

### Circumstances
- Track the “soft” issues or aggravating factors that surround a case ("alcoholism")

### Suspects
- Contextual to a case, track all suspects

### Identities
- Track multiple aliases of individuals in the system

### Arrests
- Track arrests made in course of an incident investigation
- Arrests are tied to individuals

### Victims
- Track victims in the context of offenses or incidents
Business Intelligence

Identifies Crime Trends, Patterns and Clusters

Performance metrics
• Pre-defined Executive dashboards
• ‘Real Time’, Regional Data
• Aggregate & Summary Views:
  • Comparative
  • Drill Down
  • User defined thresholds

Transactional
• Executive, Crime Analysis, and Counter Terrorism Dashboards
• ‘Real Time’, Regional Data
• Aggregate & Summary Views:
  • Crime Reports, Emergency Calls,
  • Contact Cards, Citations, Warrants,
  • Probation, Parolees, etc.
Daon/Oracle – The Open Identity Platform

- Examining the constituents of an “Open Identity Platform”
Oracle Adaptive Access Manager

• Web access real time fraud detection
• Provides online authentication security for consumers and enterprise employees.
• Strong security that ensures business is compliant with regulatory requirements:
  • Payment Card Industry Data Security Council (PCI DSC) and
  • Federal Financial Institutions Examination Council (FFIEC) for online interaction.
• Protects against attacks such as phishing, Trojans, viruses, fraudulent transactions etc.
• Used in 70 countries, 30 M people
Immigration & Customs Enforcement (ICE) Cyber Crime Centres (C3)

- Using Oracle’s COTS CRM products, database and related portal development tools, ICE combats crimes committed online and electronically, providing a new avenue through which to pursue criminals, predators and child pornographers.
- Enabled collaboration with external Law Enforcement officials throughout US - contributed to arrest of 5,400 child sex predators plus deportation of 2,000 in first year.
- Enables online access to information to help its agents combat child pornography, money laundering and trafficking of arms, drugs and stolen art as well as intellectual property rights violations.
- C3 investigates domestic and international criminal activities occurring on or facilitated by the Internet.
- Federal agents working on those cases avoid delays, log into the C3 portal, create a case, enter information about suspected targets in a case file.
- Create a summons on-line
- Nightly importation of tips (along with images & evidence) from the National Center for Missing and Exploited Children (NCMEC) enables C3 to proactively investigate leads.
- C3 requires systems featuring industry standards, sharing of info via open standards XML & high levels of security so victim information is protected and access based on authorization and need to know.
- Greater efficiencies - hours saved can be significant in terms of a child’s safety.
Intelligence Fusion Centers

- US Fed Govt post event analysis concluded that sufficient information existed such that Law Enforcement officials could have intercepted the terrorists that flew aircrafts into WTC.
  - Philosophy relies heavily on real-time information integrated into single comprehensive 360 view
- Funding & establishment of intelligence is a direct result of need for better, more integrated info. about suspects, locations etc that may be used in planning a crime, including a terrorist act
- Effective & Efficient mechanism to exchange information & intelligence
- Post 911 public sector mandated to transform from “need to know” to a “need to share” community (incl nationally sensitive info.)
- Improve ability to fight crime & terrorism by analyzing data from a variety of sources & dbs (tips, leads, driver license, vehicle reg. etc)
- Enables detection, deterrence and prevention of future terrorist attacks
- Operational configurations: regional –sharing info. among states; vertical structure –connecting states to federal agencies but not to other states.
The Concept of a Network of Networks

Defense
- Military Health Networks
- Force Support Networks
- Command & Control Networks
- Intelligence Networks

Foreign Affairs/State Department
- Diplomatic Services Networks
- Communicable Disease Monitoring Networks
- Public Health Networks

Healthcare
- Justice
- Central Judicial Networks
- Public Health Networks
- Central Police Networks

Homeland Security
- States / Provinces
- Cities/Counties/Prefectures
- Trusted Information Grid
- Diplomatic Services Networks
- Emergency Mgmt
- Fire
- Public Works
- Police/Sheriff
- Hazardous Materials
- Emergency Mgmt
- Private Sector
- Emergency Medical
- Enemies of the State

International
- Command & Control Networks
- International Police Networks

Force Support
- Transportation Departments
- State Militias
- State Police
- Public Health

Immigration
- Immigration Networks

Customs
- Customs Networks

Financial Services
- Financial Services Monitoring Networks

Natural Disaster & State of Emergency
- Natural Disaster & State of Emergency Networks

Enemies of the State Monitoring Networks

Oracle
Active Intelligence Hub

- Command & Control Center for Monitoring
  - Terrorism (physical and cyber)
  - Crisis
  - Natural disaster response
  - International criminal networks
  - Major Events

- Increasing demand for:
  - Real-time intelligence
  - Trusted information sharing
  - Rapid integration of disparate data
  - Response agility
  - Fast, reliable innovative solutions
Visualisation Integration

“Visual Search Displays the links between people, vehicles, locations, phones and a wide range of other entities, allowing investigators or frontline operatives to see the patterns in their data and progress investigations or assessments more effectively”
Visualise the Person
Information linked to an Address
Information Linked to a Phone
Value Proposition for Customer

- Enables integration of information intelligence and incident data
- Increases efficiency of criminal investigation process
- Enhances collaboration of confidential info. securely across organisation
- Focus on real threats or issues
- Enables Business Intelligence, Crime Trend Analytics, Proactive Policing, & Resource optimisation
- Embeds intelligence into business process
- Minimises admin. time & maximises patrol time for front line officers (mobility)
- Can replace several business critical applications for Law Enforcement to save $Ms in recurrent expenditure.
  - Incident Management (RMS)
  - Investigative Case Management
  - Property & Seized Forensics Evidence Management
  - Analytics that provide Crime Trends and Statistics