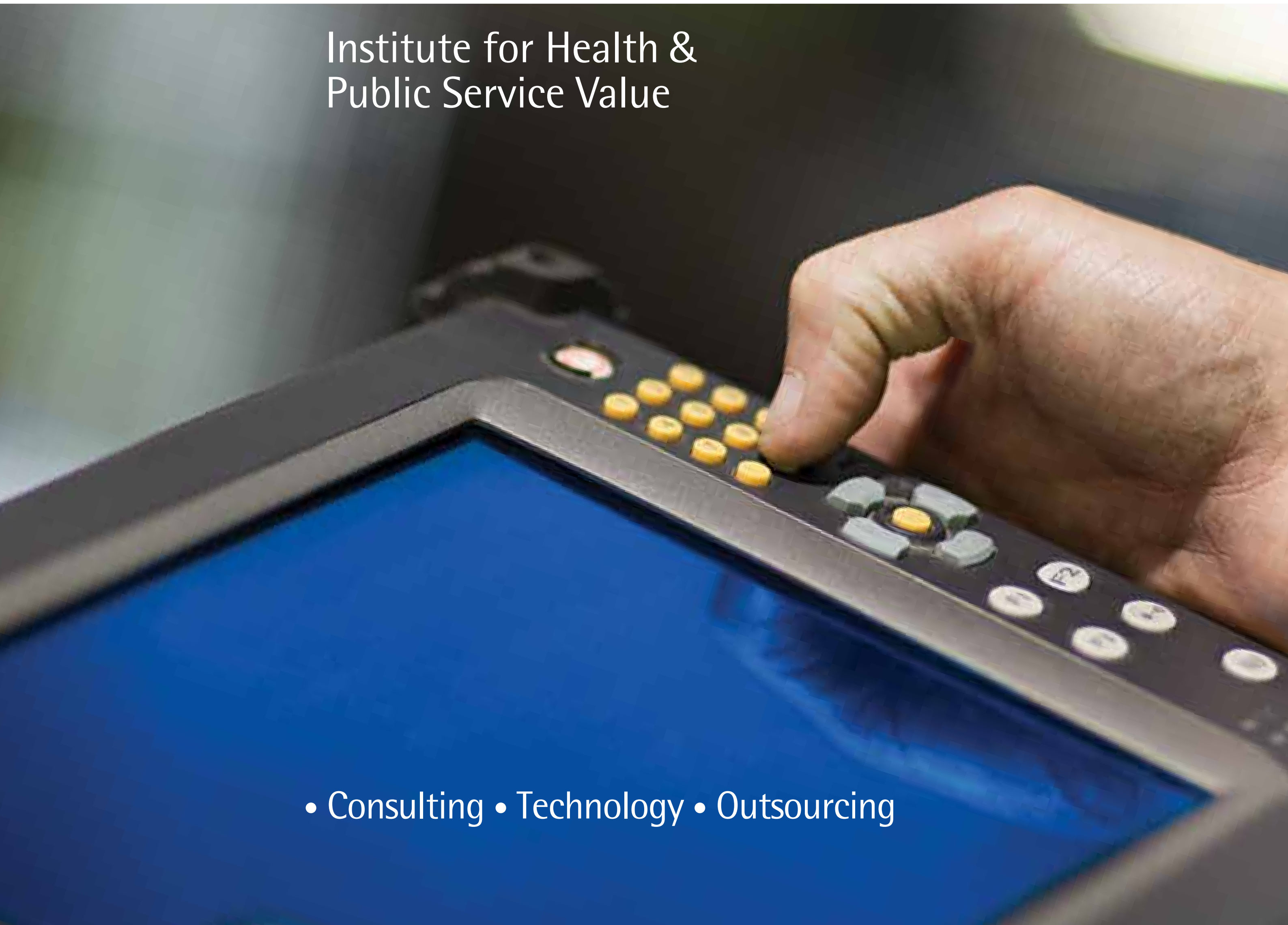
Information Management in Policing

Improving efficiency and performance by unlocking the value of information



Institute for Health & Public Service Value

• Consulting • Technology • Outsourcing

High-performance policing

Police forces around the world face unprecedented challenges: the need to tackle volume crime, address the increasing challenge posed by transnational criminal networks and deal with the ongoing threat of international and domestic terrorism. At the same time, they must meet increasing citizen expectations for more visible community-oriented policing and greater public transparency and accountability. Moreover, police forces must meet these challenges while reducing costs and resource, improving efficiency and eliminating waste.

Faced with these challenges, how are police forces to protect citizens, increase public confidence and make people feel safer?

Information management plays a crucial role in all policing activities. Effective information management enables the police to reduce costs by minimizing waste and duplication. Effective information management can, for example, remove unnecessary recording for officers, enable police forces to share services and systems, allow for better use of analytics to support cost-based decision making and ensure specialist policing skills are utilized effectively in the community.

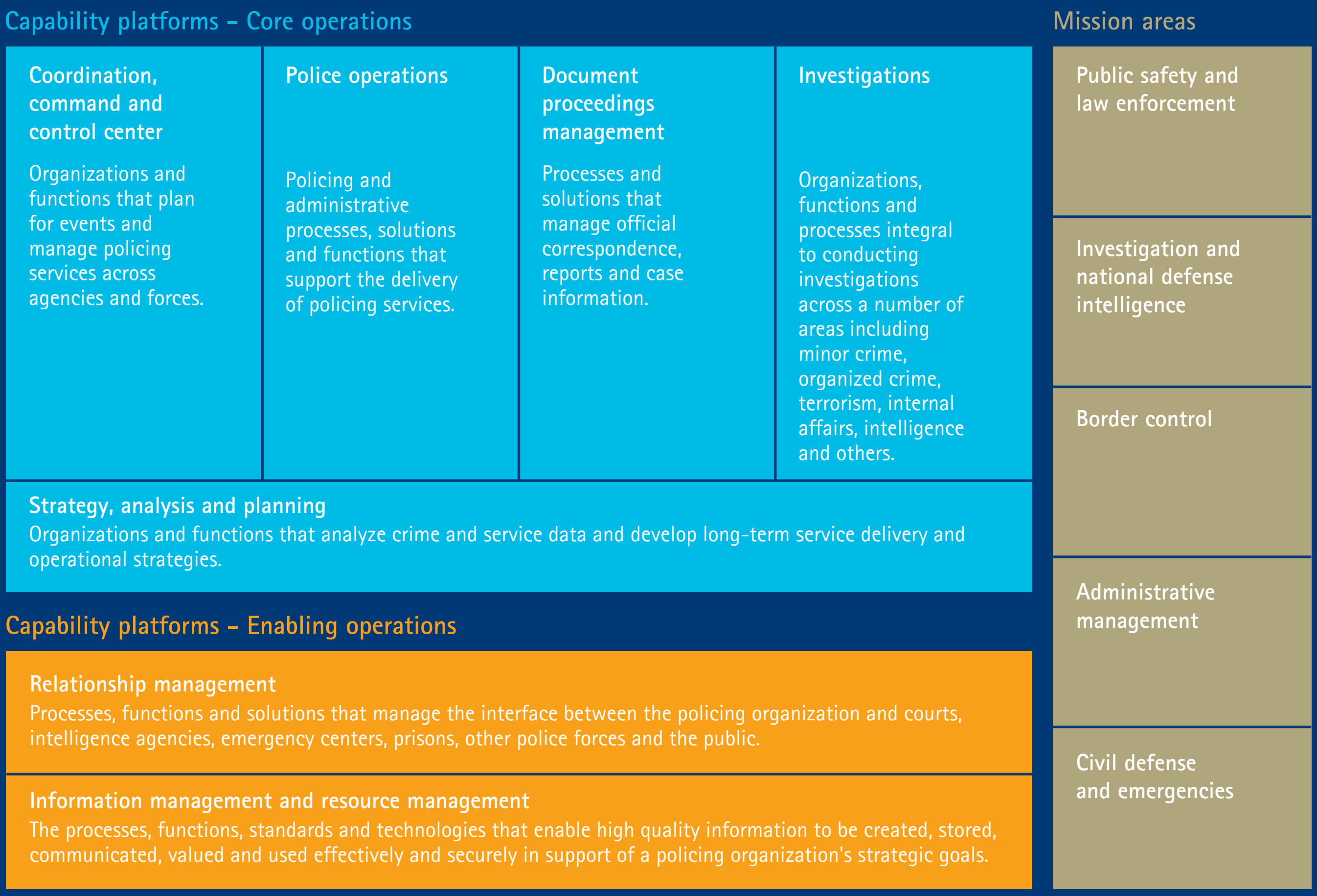
Information management also increases the effectiveness and performance of policing services in a number of ways. It enables collaboration and information sharing between police forces and other agencies, supports the use of analytics to strengthen intelligence-led and preventive policing and enables officers to access critical information remotely. It also helps the police increase public confidence by enabling them to engage with the communities they serve through tools, like crime maps, which help citizens understand policing operations and hold the police to account.

Information management encompasses the processes, functions, standards and technologies that enable high quality information to be created, stored, communicated, valued and used effectively and securely in support of an organization’s strategic goals.

Information management and policing operating models

Accenture's research and experience suggests that around 75 percent of the processes required to track and respond to crimes, however large or small, however local or international, wherever they occur, are the same. As a result, while police forces must reflect local legislative and cultural differences, it is possible to identify a core set of common policing processes. Developed by Accenture's Policing Centre of Excellence and drawing on experience working with police forces around the world, the Accenture Policing Operating Model (see figure 1) identifies a set of processes and capabilities common to all police forces. The model defines five mission areas (the services the police provide) and seven capability platforms (how the police deliver their services). Each mission area is delivered through different combinations of the various capabilities. Information management is a key element of all policing capabilities. As a result, strengthening information management will deliver significant efficiency and performance improvements across the board.

Figure 1: Accenture's Policing Operating Model



Capability platforms – Core operations

Coordination, command and control center
Organizations and functions that plan for events and manage policing services across agencies and forces.

Police operations
Policing and administrative processes, solutions and functions that support the delivery of policing services.

Document proceedings management
Processes and solutions that manage official correspondence, reports and case information.

Investigations
Organizations, functions and processes integral to conducting investigations across a number of areas including minor crime, organized crime, terrorism, internal affairs, intelligence and others.

Strategy, analysis and planning
Organizations and functions that analyze crime and service data and develop long-term service delivery and operational strategies.

Capability platforms – Enabling operations

Relationship management
Processes, functions and solutions that manage the interface between the policing organization and courts, intelligence agencies, emergency centers, prisons, other police forces and the public.

Information management and resource management
The processes, functions, standards and technologies that enable high quality information to be created, stored, communicated, valued and used effectively and securely in support of a policing organization's strategic goals.

Mission areas

- Public safety and law enforcement
- Investigation and national defense intelligence
- Border control
- Administrative management
- Civil defense and emergencies

The role of information management in policing

Information is the life blood of policing. As the Accenture Policing Operating Model (see Figure 1) shows, information management capabilities play a critical role in supporting all policing and administrative processes and enabling the delivery of policing services. Effective information management enables police forces to unlock the value of information and improve their efficiency and effectiveness by:

- Reducing the cost, in time and resources, of data collection and entry.
- Providing timely access to high-quality information held by different organizations.
- Enabling police forces to share high-quality information securely and effectively with partners.
- Feeding business and performance analytics that deliver insight to enable improved decision making and resource allocation.
- Supporting data aggregation and intelligence analysis that turns information into actionable intelligence, thereby enabling the identification of links between people, objects, locations and events and a single-view of an individual, group or network.

All policing activities should be underpinned by robust information management to ensure the effective use of resources and data assets.

However, the police face a range of challenges associated with the creation, collection, storage, communication, valuation, sharing and use of data (see Figure 2). Unless properly addressed, these challenges reinforce data silos, inhibit collaboration and hinder data access. They can prevent the police from unlocking the value of the information they hold and undermine improvements in efficiency and performance. To address these challenges, the police must develop robust information management capabilities.

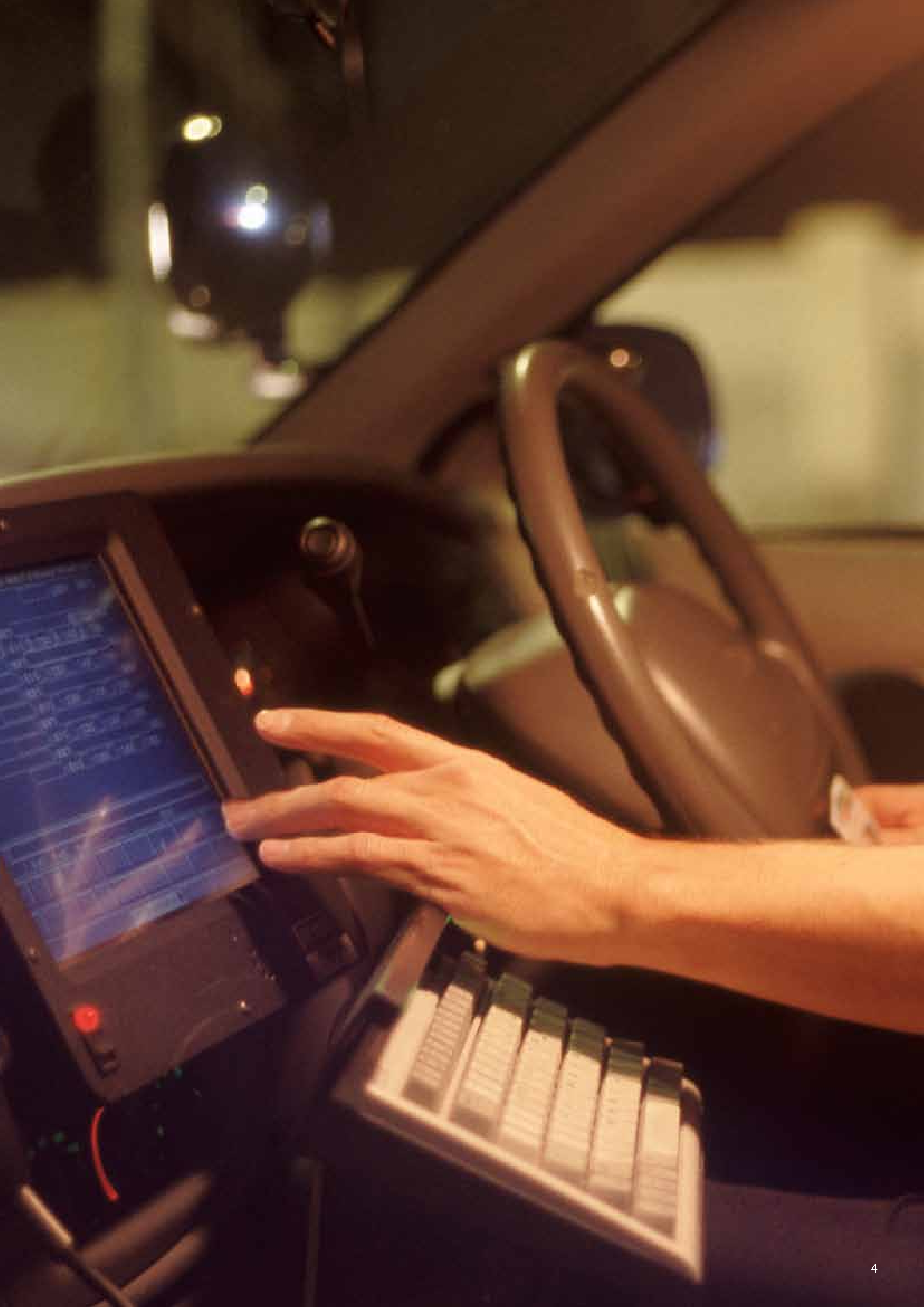


Figure 2: Critical information management challenges

Collecting information

To reduce time spent on administrative tasks and maximize information collection, police forces must enable remote access to enterprise IT systems, ensure single-point data entry, digitize paper-based records and deploy effective automated data-capture solutions.

Accessing information

To improve the effectiveness of policing services, police forces must ensure that officers can access the right information at the right time. To achieve this, users must be able to access enterprise IT systems remotely and locate information efficiently in highly distributed environments

Sharing information

To enable collaboration with public, private and non-governmental organizations and ensure the accuracy and completeness of information, police forces must be able to share information effectively and securely with other organizations. Effective information sharing requires the ability to exchange data in different formats and search for data stored in systems outside the organization. Effective information sharing also requires openness to sharing information outside the organization and a willingness to break down traditional information silos.

Ensuring the quality of information

To realize the value of enterprise IT systems, information they make available must be accurate and meaningful so it can be used for its intended purpose. To ensure high-quality data, police forces must enforce common data-entry standards. These standards should be supported by applications configured to encourage desirable user behaviors. Ensuring data quality in distributed environments also requires solutions that maintain the integrity of data communicated between systems in messages.

Protecting and securing information

To ensure compliance with legislative and regulatory obligations and to maintain data quality and prevent data breaches, police forces need effective enterprise security architectures. Effective enterprise security architectures proactively manage security risks, effectively identify and prioritize threats, and rapidly address vulnerabilities across organizational and information silos. Data security also requires users to follow robust data-handling and security policies to minimize the risk of unauthorized system or data access. Access control models and solutions must prevent unauthorized access, record access requests and assign appropriate permissions to users based on real-world job functions.

Complying with legislative, regulatory and best practice guidelines

To ensure compliance with data security, data management, auditing and operational guidelines, police forces require a coordinated approach across organizational and information silos that enables IT, policing, administrative and management functions to collaborate effectively. This coordinated approach minimizes the cost of compliance and ensures a more effective, flexible compliance architecture.

Maximizing the value of information

To improve the performance of policing services, increase the efficiency of policing and administrative processes and strengthen cost-based decision making, police forces require effective analytics solutions. These solutions translate information into actionable intelligence, enabling intelligence-led and predictive policing.

Developing effective information management

To unlock the value of information, the police must develop workforce and process capabilities that enable efficient, effective and secure information collection, storage, use and sharing.

In the past, police forces have generally adopted a siloed and tactical approach to information management. They have allowed organizational and information silos to overcome information management challenges on an ad-hoc basis. While it is important for police forces to address issues as they arise, this fragmented and reactive approach to information management significantly increases the cost of information management and reduces its effectiveness and flexibility.

The Accenture Information-Management Framework for Policing provides a complete model for information management and is designed to help police forces design more effective information-management architectures.

Accenture recommends a collaborative, strategic and enterprise-wide approach to information management. To achieve effective information management, police forces must develop a consolidated information-management architecture—a layer of processes, functions, policies and solutions that ensure the effective and secure creation, collection, storage, communication, valuation, sharing and use of information. Effective information-management architectures integrate disparate information, security, access control and content-management capabilities and include policing, administrative and technology work streams. Enterprise IT systems are an integral part of effective information-management architectures because they provide the IT services, data stores, standards, frameworks and processes required to support secure data and process interoperability across organizational boundaries.

The Accenture Information-Management Framework for Policing (see Figure 3) provides a complete model for information management and is designed to help police forces design more effective information-management architectures.

An information-management architecture is a layer of processes, functions, policies and solutions that ensure the effective and secure creation, collection, storage, communication, valuation, sharing and use of information.

Developed by Accenture professionals and drawing on experiences of system implementations around the world, the framework divides information management into five highly-interrelated disciplines:

- Utilization
- Accessibility
- Sharing
- Quality
- Security

Each discipline has multiple components—the most important processes, functions and technologies required to unlock the value of information.

Figure 3. The Accenture Information Management Framework for Policing

	Information-management disciplines	Components
Information management	**Utilization** Transforming information into actionable insight and intelligence to improve strategic, operational and cost-based decision making	Analytics
		Data visualization
		Information flow optimization
		Mobile and remote data entry and access
	Accessibility Ensuring secure and efficient access to information held in highly distributed environments across different systems	Access control
		Data discovery
		Enterprise search
	Sharing Enabling police forces to collaborate and share information efficiently and effectively within and beyond their organization	Technical interoperability
		Data interoperability
		Process interoperability
		Interoperability governance
	Quality Ensuring information is meaningful, accurate, internally consistent and can be used for its intended purpose	Data entry
		Error correction and data validation
		System and interface certification
		Standards-driven architecture and standards management
	Security Preventing data corruption and unauthorized access	Data-security and data-handling policies
		IT security audit
		Network integrity
		System hardening

Utilization

Police forces have access to a huge amount of information. The challenge is transforming this information into actionable intelligence to improve strategic, operational and cost-based decision making. Analytics and visualization tools can extract aggregated information from data and communicate this information graphically to support decision making and intelligence-led policing.

To maximize the value of analytical insight, police forces must ensure that decision makers have timely access to relevant information at the point of need. To ensure data is utilized effectively, information-management architectures must include four components:

Analytics – solutions that use quantitative, statistical and exploratory analysis and predictive modeling to generate meaningful information and actionable insight from data that may be unstructured or stored in various locations. Business analytics can be used to improve the efficiency of administrative processes and strengthen cost-based decision making. Analytics can also improve the performance of police forces by strengthening intelligence management, enabling officers to anticipate crime and supporting targeted crime prevention strategies.

Data visualization – solutions that represent data graphically so large volumes of information can be communicated, interpreted and acted upon efficiently. Data visualization tools can be used to identify links between people, objects, locations and events. They help map crime patterns, communicate and analyze performance and evaluate process efficiency and the distribution of resources.

Information flow optimization – process re-engineering programs that identify where and when information is required in policing and administrative processes and re-configure information flows to ensure that accurate, targeted information is made available to those that need it in a timely way.

Mobile and remote data entry and access – mobile and remote solutions that enable location-independent access to enterprise systems so users can enter and access data on the move. Mobile applications must be easy to use, provide access to large volumes of information efficiently and have sufficient functionality to meet a diverse range of needs. Mobile solutions improve the efficiency and effectiveness of police forces by reducing the amount of time officers spend away from the frontline and improving their direct access to information.

Accessibility

Policing information is generally held across different systems operated by a range of organizations. These organizations include those within criminal justice, national security, and local and central government as well as other international policing organizations. Ensuring secure and efficient access to this information requires enterprise IT systems and processes that grant permissions to users based on real-world job functions, prevent unauthorized access, locate and organize data in complex environments and enable users to search for information stored in different systems.

To ensure secure and efficient data access, information-management architectures must include three components:

Access control – role-based access control models that grant permissions to users based on real-world job functions, and solutions that prevent unauthorized access to data. Ensuring users can access vital information while maintaining data security is a complex challenge, particularly in distributed environments with several different access control models.

Data discovery – solutions that locate and organize data so organizations know where data assets are stored and are better able to monitor, manage, protect and access them. Effective data discovery is very important for police forces that need to manage high volumes of unstructured data from a wide range of sources.

Enterprise search – solutions that enable users to search for information stored in a variety of locations. Effective enterprise search solutions will retrieve data from a wide range of sources, enable users to enter complex search queries and return a consolidated list of information resources ranked by relevance. Enterprise search solutions enable a single view of people, objects, locations and events by allowing officers to access information held by a number of different organizations.

Sharing

The growing complexity of modern policing requires police forces and other organizations to collaborate and share information more efficiently and effectively. Effective data sharing requires a sufficient level of interoperability between systems and organizations. In broad terms, there are three categories of interoperability:

- Technical interoperability – systems are able to exchange data.
- Data interoperability – systems are able to automatically process and display data exchanged between them.
- Process interoperability – organizations are able to use shared information effectively.

Achieving and maintaining interoperability between systems and organizations requires common governance processes that deploy, enforce and manage interoperability standards. To ensure effective data sharing, information-management architectures must include four components:

Technical interoperability – infrastructures, network solutions and communication protocols that enable systems to communicate and receive data. A high level of technical interoperability enables systems to share large volumes of data efficiently and reliably and increases system flexibility. Technical interoperability is the lowest level of interoperability as it only involves the sharing of data and not the processing or display of that data.

Data interoperability – data standards that enable data and information communicated between systems to be automatically processed and displayed. A high level of data interoperability requires standard data models to ensure data is structured consistently and common ontologies to ensure concepts and relationships between concepts are defined consistently. Data interoperability enables systems to accurately interpret the content and meaning of data and information communicated between them.

Process interoperability – collaborative workflows, common data-entry standards and shared information flows that enable organizations to use shared information to strengthen decision making and improve administrative and policing processes. Process interoperability enables organizations to maximize the value of technical and data interoperability.

Interoperability governance – a function that works across organizational and information silos to develop, manage and enforce common standards, protocols and processes to enable technical, data and process interoperability. Effective interoperability governance increases the breadth and depth of data sharing by increasing the number of information and organizational silos able to share information and the level of interoperability between those silos.

Quality

Police forces must manage very high volumes of data from a wide range of sources. Ensuring the quality of that data is critical. High-quality data is meaningful, accurate, internally consistent and can be used for its intended purpose. Data integrity—the validity, accuracy and reliability of data after it has been stored, transferred, retrieved or processed—has a significant impact on data quality. Poor-quality data can undermine the performance and efficiency benefits of enterprise IT systems and data sharing. As a result, it is vital that police forces maintain and improve data quality. They can do this by implementing training programs, communications strategies and performance criteria that encourage accurate and complete data entry and by putting solutions in place that prevent, detect and correct data errors and preserve data integrity.

To maintain and improve data quality, information-management architectures must include four components:

Data entry – policies, training and applications that minimize user-generated errors at the point of entry and ensure accurate and complete data entry. By deploying user friendly, intelligent and mobile data-entry solutions, police forces can improve the efficiency of data entry while improving data quality.

Error correction and data validation – manual and automatic processes that detect and correct errors in information, and validation rules that verify that data conforms to format, quality, integrity, accuracy and structure specifications. Enforcing common error-correction processes and data-validation rules across systems and organizations that share information increases data quality by reducing errors in data communicated between systems.

System and interface certification – roles, processes and solutions that verify that systems and interfaces conform to specifications defined by regulators, IT governance organizations and Standards Development Organizations (SDOs). Ensuring systems and interfaces conform to common specifications maintains the integrity of data as it is processed and communicated between interoperable systems.

Standards driven architecture and standards management – system architectures that use common standards for the collection, storage and processing of data, thereby promoting a high level of data quality through similar data processing across component systems. Standards management includes the roles, processes and solutions that develop, manage and enforce common technical, communication, messaging and data standards. Standards management enables subsystems to share high quality information

Security

Preventing data corruption and, more importantly, unauthorized access to data are critical issues for the police as they hold and manage high volumes of sensitive information. Data security must be a priority for police forces because data breaches significantly undermine public trust and confidence, are a major compliance issue, can have a detrimental impact on performance and in some cases result in the loss of life. Ensuring data security requires police forces to develop policies, processes, functions and solutions that proactively manage security risks, effectively identify and prioritize threats and rapidly address vulnerabilities.

To ensure data security, information-management architectures must include four components:

Data-security and data-handling policies – policies that minimize information-security risks and prevent unauthorized access to information by encouraging users to be security conscious. Effective data-security and handling practices include:

- Collecting, storing and sharing data securely using appropriate security technologies, such as encrypted storage devices and secure communication channels.

- Minimizing the risk of data loss or misuse by maintaining the effectiveness of access controls—for example, not sharing passwords and ensuring that passwords meet certain criteria.

- Proactively identifying and minimizing security and confidentiality risks.

- Reporting security breaches and unauthorized or improper use of information.

- Restricting physical access to hardware—including laptops, desktops, mobile devices and mobile phones—that store or enable users to access sensitive data.

- Educating other users to raise awareness of data-security and data-confidentiality risks and encouraging them to be security conscious.

IT security audit – manual and automatic processes that test and evaluate the effectiveness of IT systems' information security measures. IT security audits ensure that data is properly protected from unauthorized access, that all relevant security threats and vulnerabilities have been identified, and that data-handling processes are correctly configured to minimize security risks. IT security audits may be conducted by a third party and typically include a number of components. Among them: compliance verification, security-standards certification, security assessments, penetration testing and user-awareness testing.

Network integrity – solutions and functions that enable networks to maintain expected functionality, performance and service availability despite unexpected events, such as security threats and spikes in demand. A high level of network integrity ensures the availability of processes and services that maintain data security across the network. Network integrity solutions should automatically detect and address security threats and unwanted network traffic, preserve network bandwidth by managing and prioritizing legitimate traffic and generate reports on network performance to help network administrators manage networks more effectively.

System hardening – periodic or ongoing processes that reduce security risks by evaluating the effectiveness of security architectures, identifying security risks and undertaking security improvements—including removing vulnerable and unnecessary services and applications and updating security configurations and access controls.

Information management in practice

Crime prediction and prevention

To improve the performance and efficiency of policing, police forces around the world are developing preventive, evidence-based policing strategies and focusing on intelligence-led policing. This means deploying resources to the right place at the right time, identifying and addressing key causal factors of crime, focusing on measuring public safety outcomes rather than outputs, and closely aligning organizational strategy with changing crime trends. Intelligence-led and predictive policing requires analytics. Analytics aggregates data from a number of different sources and uses statistical analysis and predictive modeling to identify crime trends and highlight "hidden" connections between disparate events and trends. This provides a 360 degree view of crime, enabling police forces to predict the pattern of future criminal behavior and identify the key causal factors of crime.

Police forces across the US are using analytics to support intelligence-led policing and improve the efficiency and effectiveness of their operations. For example, in 2006 the City of Richmond Police Department deployed an advanced data-mining and predictive analytics solution. The results: between 2006 and 2007 the city's homicide rate dropped 32 percent, rapes declined 19 percent, robberies fell 3 percent, and aggravated assaults were down 17 percent. In 2008, crime rates continued to fall: homicides declined a further 40 percent, rapes by 8 percent, robbery by 20 percent, and aggravated assault by 5 percent. Similarly, the Memphis Police Department has used predictive analytics to improve the efficiency and effectiveness of policing. Between 2006 and 2010, serious crime in Memphis fell by more than 30 percent, which includes a 15 percent reduction in violent crimes.

Data-Driven Approaches to Crime and Traffic Safety (DDACTS) is a law enforcement operational model that integrates location-based crime and traffic crash data to determine the most effective methods for deploying law enforcement and other resources. Using geo-mapping to identify "hot spots"—areas of high incidence of crimes and crashes—DDACTS uses targeted traffic enforcement strategies to fight crime and reduce crashes and traffic violations. DDACTS initiatives across the United States are supported by a partnership between the US Department of Transportation's National Highway Traffic Safety Administration and two agencies of the US Department of Justice. DDACTS is driving real improvements in the effectiveness of policing services across the United States. For example, Lafourche Parish, Louisiana, has seen crime and crash rates decrease significantly only one year into their DDACTS program: the number of fatal drink-driving crashes fell from 27 in 2008 to 11 in 2009; drink-driving arrests increased from 150 in 2008 to 300 in 2009 and the overall crash fatality decreased 59 percent in 2009. These improvements are principally the result of improved resource

management. Using an evidence-based approach to resource deployment, the Sheriff's Office was able to target resources in locations with the highest crime and crash rates; improving the effectiveness of policing services without incurring additional cost.

Mobile data and systems access

Police forces around the world are investing in developing and deploying integrated mobile solutions that enable remote access to critical information assets and enterprise IT systems. These solutions allow officers to access information on people and vehicles, communicate with other law enforcement agencies, submit forms and generate and share intelligence reports without returning to the station.

Mobile technology is having a significant impact on the efficiency and effectiveness of policing services in the United Kingdom. For example, by rolling out smart phones, Bedfordshire Police have reduced the proportion of time an officer spends in a police station from 46 percent to 36 percent, while increasing police visibility within the region by over a third. Similarly, in the United States, local law enforcement organizations are rolling-out the Mobile and Wireless Multi-Modal Biometric Offender Recognition and Information System (MORIS): a handheld biometric device based on the iPhone that enables officers to identify suspects and retrieve their criminal records in seconds using electronic fingerprinting, iris scanning and facial recognition.

Data visualization

Data visualization solutions enable officers and citizens to identify patterns and trends in crime, and police force performance and operations by aggregating data from a variety of sources and communicating it graphically or topographically. These solutions include Graphic Information Systems (GIS), mash-ups that overlay crime and/or police information on interactive maps, two and three-dimensional link chart visualizations that automatically display connections between people, places, events and objects, temporal charts that highlight crime trends and crime clusters and dashboards that visualize real-time and trend performance and response data.

Operations-focused data visualization solutions can improve the efficiency and effectiveness of policing services by highlighting poor performance or inefficiency and strengthening evidence-based and preventive policing strategies. Citizen-focused data-visualization solutions can communicate crime statistics and police performance to the public. This can be effective in strengthening public confidence in the police and encouraging citizens to play a more active role in improving public safety in their community by working with the police, for example by reporting suspicious behavior and establishing neighborhood watch schemes.

Crime-mapping solutions are very common across the United States.

Crime-mapping service providers, such as crimemapping.com, crimereports.com and the Omega Group provide hundreds of public safety and law enforcement agencies with operations- and citizen-focused crime-mapping solutions. Seattle's My Neighborhood Map is one of the most advanced citizen-focused crime-mapping solutions available. My Neighborhood Map maps crimes, enables easy "one-click" access to redacted crime reports and also maps emergency incidence response data. This provides citizens with a comprehensive view of crime in their area and enables them to evaluate the effectiveness of police responses.

Data sharing and collaboration

The benefits of data sharing and aggregation are wide ranging and include improved performance of police forces, reduced administrative costs, improved first response and crisis management capabilities, and more effective evidence-based policing and intelligence management. Moreover, secure and effective information sharing enables the police to develop predictive analytics and data visualization solutions that are critical to intelligence-led policing. To achieve these benefits, police forces around the world are establishing local, regional and national police information networks that enable secure and effective information sharing between law enforcement, public safety, criminal justice and other relevant organizations.

In the United States, some states are developing flexible, scalable and cost-effective state-wide information networks that enable secure and effective information sharing across jurisdictions. For example, 27 law enforcement agencies across Colorado use a secure internet-based solution to share information. The solution connects disparate systems in a distributed environment and automatically transposes data held by different agencies' systems into common code standards so it can be shared effectively. In Ohio, over 725 of the 900 local law enforcement agencies share information through the Ohio Local Law Enforcement Information Sharing Network (OLLEISN), a secure internet-based solution that enables officers to search a single database containing information from all participating agencies' Computer Aided Dispatch (CAD)/Records Management Systems (RMS). OLLEISN uses common data, technical and security standards to enable information exchange between disparate CAD/RMS systems so agencies are able to deploy systems that best meet their needs while realizing the benefits of effective information sharing.

To address complex transnational crime, the international law enforcement community is increasingly sharing information through Interpol's data services and databases. Interpol, the world's largest international police organization, facilitates cross-border police cooperation in part by providing police forces with an infrastructure that enables them to share information internationally. Interpol provides all its member countries with instant, direct access to a wide range of criminal information including missing persons, known international criminals, stolen and lost travel documents, stolen motor vehicles and works of art, DNA profiles and fingerprints. All databases, except the one of child sexual exploitation images, are accessible through the I-24/7 Dashboard, a restricted-access Internet portal. An automated search facility enables member countries to conduct simultaneous searches across a number of databases.

Interoperability

Enabling police forces, criminal justice agencies and other organizations involved in public safety to share information securely and effectively is a priority in many countries. However, secure and effective data sharing requires a high level of interoperability between systems and processes within highly distributed environments. To achieve sufficient interoperability, countries around the world are undertaking programs to develop common standards and governance processes that will drive the adoption of common interoperability standards across the public safety system.

In the United States, the Department of Justice (DOJ), through various agencies and workgroups, is increasing data sharing across US law enforcement and public safety organizations. It is achieving this through a number of programs that promote and enable interoperability between disparate systems and organizations at local, state and national levels:

Fusion centers and intelligence sharing – fusion centers bring together all relevant public safety, law enforcement and private organizations involved in preventing and responding to criminal and terrorist activities. Fusion centers provide "effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources." To achieve technical, data and process interoperability between different organizations, fusion centers focus on designing and embedding "processes through which information is collected, integrated, evaluated, analyzed, and disseminated." Working with a wide range of stakeholders through the Fusion Center Focus Group, the US Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) has helped develop a set of 18 detailed guidelines to help agencies establish successful fusion centers and achieve a high level of interoperability between systems and organizations. These guidelines are wide-ranging and touch on every aspect of achieving technical, data and process interoperability including governance, interconnectivity, workforce issues, processes and infrastructure.

Justice Reference Architecture (JRA) – developed by Global's Infrastructure/Standards Working Group in collaboration with the DOJ's Office of Justice Programs, Bureau of Justice Assistance, JRA is a reusable information-sharing solution specific to the justice domain. It is designed to enable the reuse of established best practices in IT architecture and design and thereby cut 80 percent of implementation time and cost for state and local justice agencies. The JRA has four components: Reference Architecture Planning, Service Specification Packages, Technical Implementation Guidelines and Policy Guidance. Together, these components provide a comprehensive, replicable, and scalable solution that enables technical and data interoperability across disparate systems.

National Information Exchange Model (NIEM) – developed by the US Department of Justice and the Department of Homeland Security and launched in 2005, NIEM is a platform designed to "develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies". NIEM enables seamless information exchange between disparate systems by:

- Bringing stakeholders and other interested parties together to identify information-sharing requirements in day-to-day operational and emergency situations.
- Developing standards, a common lexicon and an online repository of information-exchange package documents to support information sharing.
- Providing technical tools to support development, discovery, dissemination and re-use of exchange documents.
- Providing training, technical assistance and implementation support services for enterprise-wide information exchange.

NIEM enables technical and data interoperability by providing a standardized data model, which includes a data dictionary and a reference schema, as well as the concepts and rules that underlie its structure, maintain its consistency, and govern its use.

Developing an effective information strategy

High-performance police forces must develop operating models that enable them to provide more effective policing services, improve public trust and confidence in the police, increase transparency and accountability and reduce costs. Effective information management capabilities are a key enabler in improving efficiency and performance because they enable police forces to unlock the value of information. To strengthen their information management capabilities, police forces should develop consolidated enterprise-wide information-management architectures.

The critical first step in designing and deploying an effective information-management architecture is to develop an information strategy. The strategy should define a set of common information principles and include policies, frameworks and guidance to support the adoption of these principles across organizational and information silos. The aim: to embed a common set of information-management standards and practices that enable high-quality information to be created, collected, stored, communicated, valued and used effectively and securely in support of the organization's strategic goals. Adopting a comprehensive, structured approach to information management, such as the Accenture Information Management Framework for Policing (see Figure 3), will help ensure police forces develop effective information strategies that improve the efficiency and performance of policing services.

Based on research and experience working with police forces around the world, Accenture has defined a set of good practice recommendations for police forces developing an information strategy:

Involve a wide range of stakeholders

An effective information strategy will cut across organizational silos and will impact operational, technology and strategic functions. Information strategies should be developed and refined through a collaborative process that brings together different perspectives from across a range of functions including front-line officers, technologists, senior officers, administrators and key decision makers.

Establish a central governance function

To ensure that common information management standards and practices are adopted across the organization, an information strategy should establish a strong, central governance function responsible for:

- Managing communications and raising awareness.
- Delivering education and training.
- Disseminating guidance and good practice.
- Developing and enforcing technical standards such as data models.
- Supporting the development and implementation of key policies such as data-entry standards for officers, information-sharing protocols and data-security and privacy guidelines.

Align the information strategy with key strategic priorities

To help ensure that improvements in information management will have a significant impact on efficiency and performance, an organization's information strategy should explicitly link with its strategic priorities. For example, if the organization is targeting cost reductions, the information strategy should identify means of reducing waste and duplication, enhancing the efficiency of operations and providing decision makers with insight that strengthens cost-based decision making.

Do not neglect the cultural and organizational dimensions of information management

Improving the effectiveness of information management requires cultural and organizational change as well as new information systems. There are three main cultural and organizational dimensions to information management that should inform an organization's information strategy:

- Training and education – ensuring that users understand how to use IT systems effectively to improve efficiency and performance.
- Policing and business processes – redesigning policing and business processes to maximize the value of IT systems and enable greater collaboration and information sharing.
- Culture – creating a culture that encourages desirable practices, such as complete and accurate data entry, and ensures that the organization views information as a valuable strategic asset.

Information is at the heart of modern policing and police forces therefore rely upon effective information management. As a result, strengthening information management is a critical element in increasing the efficiency and effectiveness of police forces. Improvements in information management will drive and support improvements across the board by providing police forces with timely access to high-quality, accurate and relevant information that strengthens decision making and improves operational performance.

Contacts

Maurice Philogene
United States Policing Lead
maurice.philogene@accenturefederal.com
+1 571 414 3124

James Slessor
United Kingdom Policing Lead
james.w.slessor@accenture.com
+44 20 7844 5753

Manuel Sanchez Lopez
Police Centre of Excellence Lead
manuel.sanchez.lopez@accenture.com
+34 91 546 9234

Project Team

James Slessor
United Kingdom Policing Lead

Giles Randle
Researcher, Institute for Health
& Public Service Value

About the Accenture Institute for Health & Public Service Value

The Accenture Institute for Health & Public Service Value is dedicated to promoting high performance in the health care sector and in public service delivery, policy making and governance. Through research and development initiatives, the Institute aims to help health care and public service organizations deliver better social, economic and health outcomes for the people they serve. Its home page is www.accenture.com/healthpublicservicevalue

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with approximately 204,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$21.6 billion for the fiscal year ended Aug. 31, 2010. Its home page is www.accenture.com.

ACC10-2150 / 11-2401

1 2 4 5 8 2 6 0