High performance. Delivered.

Confederation of Indian Industry

Better information leads to better internal security

Driving High Performance in Internal Security

A CII and Accenture Report

• Consulting • Technology • Outsourcing

Contents

Foreword

From CII

The term "security" has become so complex and comprehensive that leaving anything out of its purview is simply not possible. If nothing can be left outside the ambit of security, policies and strategies should be framed keeping the future requirements in mind and not merely looking at current scenario. In order to meet the present and futuristic requirements of the security forces, a consistent approach with long term planning will yield desirable results. The long term planning also entails a larger role for industry, with special attention to research and development and greater emphasis on integrating technologies for security requirements. In a nutshell, there is a need to link the economy with science and thereby enhancing security preparedness.

It is important to respect human freedom and rights while ensuring the best internal security. Technology is an enabler and can be integrated in the internal security apparatus in a manner which will not compromise internal security preparedness by increasing its vulnerability to the cyber attacks and other unforeseen threats. Advanced technology can help investigators discriminate between criminals and regular citizens. Technology has also helped in maintaining voluminous records and mining the right kind of information. Although technology is of a greater assistance to maintain law and order, the human dimension can never be written off.

CII is an ardent advocate of a self-reliant domestic manufacturing base for sophisticated security technologies. The greater the economic base of the country, the higher security threats will be. There cannot be a blanket approach to dealing with threats. Therefore, the threat mitigation strategy should be multi-pronged. In the first place; it should be pre-emptive in nature. Second; it should be proactive. Third; it should reflect "unity of efforts" with all stakeholders on board. Fourth; minimum collateral damage through surgical strikes, wherever applicable. Lastly; the strategy should be comprehensive enough to ensure cessation of recurrence of the trouble.

This CII and Accenture report on "Better Information Leads to Better Internal Security Management," aims to articulate a workable solution to address internal security challenges. A right stride encompassing the above strategy with greater involvement from industry can lead India to a level where it can play a significant role – not only domestically but also regionally and globally. The ongoing modernisation plans and increased scope of offsets to internal security and civil aviation have enhanced the scope of industry participation in the internal security scenario.

CII has and will continue to suggest workable solutions to policy-makers; explore opportunities for the industry in hassle free technology-based and integrated intelligence solutions for internal security requirements. We will continue to support our security forces in whatever manner possible.

Gurpal Singh

Deputy Director General & Head Defence,
Aerospace & Security Confederation of Indian Industry

Foreword

From Accenture

Recent terrorist plots and events across the world regularly remind us of the significance of information in our ever-shrinking, dynamic world. Every day, internal security agencies are tasked with developing real, pursuable leads from a mountain of data. Since incomplete and imperfect data is the norm in this complex security environment, security agencies often spend valuable time on dead-end leads—trying to decipher essential information that might enrich a case quickly and help in a critical investigation.

Security agencies face a dynamic and rapidly evolving environment that requires them to collect and process data from a broader range of sources and at a faster pace than ever before. In the future, agencies will continue to be challenged to acquire, identify, integrate, analyze and disseminate relevant information to achieve high performance.

Intelligence-led law enforcement - a proven model of internal security management in which information serves as a guide to operations - arms internal security agencies with powerful tools that can help them identify and respond to emerging threats quickly and effectively. Although information is the first line of defence against crime, sharing it is never easy. Cross-agency or cross jurisdictional involvement can decentralize critical data and the lack of standardized technology platforms isolates it further.

For implementing intelligence-led law enforcement, security agencies need to leverage advanced IT based information gathering and analysis platforms that facilitate integrated knowledge modelling. These systems should possess robust investigation capability without compromising on scalability and ease of customization. It is imperative that such systems combine leading search and visualization components into a single solution to help the law enforcement community discover, manage and share actionable information. This innovative investigative capability requires amalgamation of strategy, process and technology to improve the quality and reliability of knowledge discovery.

Accenture has worked with security agencies to provide them access to a comprehensive range of technology assets, tools, resources and skilled consultants, many of whom are acknowledged experts in public. Accenture has been helping internal security agencies across the world to develop a culture of collaboration that allows them to operate as a cohesive, public safety enterprise starting with technology infrastructures that improve communication and information sharing. For instance, Accenture worked with the UK's Ministry of Justice (MoJ) on a project known as LIBRA. The project aimed at modernizing the UK magistrate's courts by replacing numerous local legacy systems with a new centrally-hosted web-based case management system. Accenture, in collaboration with leading technology vendors, has also developed the Accenture Knowledge Discovery Capability for integrated knowledge modelling, link analysis and discovery to assist with the law enforcement community's move to intelligence-led policing and high performance.

This report offers insights on the ways information management can be strengthened so as to protect national interests and safeguard citizens in the face of significant security threats.

Krishna Giri

Managing Director,
Management Consulting – APAC Health & Public Services

Executive Summary

Internal security agencies in India and abroad face unprecedented challenges: the need to tackle crime, address the increasing challenge of transnational criminal networks and the ongoing threat of international and domestic terrorism, cyber crime, money laundering, narco-terrorism and human trafficking. In parallel, they must meet increasing citizen expectations for more visible community-oriented law enforcement and greater public transparency and accountability. Moreover, security agencies must meet these challenges while reducing costs and resources, improving efficiency and eliminating waste.

Over the past decade, India's internal security landscape has seen dramatic changes. Given these changes and the complex security environment, the Ministry of Home Affairs (MHA) has already been at the forefront of strengthening the national security apparatus and communication and information management systems. These initiatives include establishment and operationalisation of regional NSG hubs, operationalisation of intelligence exchange between the Multi-Agency Centre (MAC) and its state level subsidiaries (SMAC), and the establishment of the National Intelligence Grid (NATGRID) among other initiatives. These initiatives need sophisticated systems for intelligence gathering and analysis and internal security operations management.

The need of the hour is effective and intelligent information management. Effective information management enables security agencies to reduce costs by minimising waste and duplication and using information gathering resources more efficiently. This can remove unnecessary recording, enable security agencies to share services and systems, help create intelligence from disparate pieces of information, allow for better use of analytics to support decision-making and ensure specialist law enforcement skills are utilised effectively in the community.
The best, actionable and prompt intelligence on internal security often comes from police stations.

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

The Role of Information in Managing Security

The role of information management

Historically, internal security and intelligence agencies have developed large and fragmented legacy systems that have resulted in "islands of information". This has hampered the exchange and analysis of information and made it difficult for them to provide the right information, while criminals become increasingly sophisticated. This has led governments to look for new and better ways to utilise the information assets they already possess.

For security agencies to be intelligence-led in protecting the public, preventing crime and bringing criminals to justice, they must have an effective and robust management of information. It is vital for security agencies anywhere in the world to manage and disseminate this information to better equip personnel from security, law enforcement, immigration, customs and intelligence agencies. With the availability of advanced technologies and communication devices, there is no scarcity of obtaining and communicating this information.

The US joint inquiry by the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence into activities before and after the terrorist attacks of September 11, 2001, presented findings under three categories, "Factual Findings", "Systemic Findings" and "Related Findings". The findings in each of these categories could be construed as saying that there was a huge amount of information that was amassed from various intelligence sources prior to 9/11 but that the information was not analysed to find actionable patterns and important links and connections were missing. Even if connections were established, those connections were not followed-up and shared across the whole intelligence community. The volume of intelligence information was not analysed to the extent that it could lead to the identification of time, place and nature of the attacks planned for September 11, 2001.

The findings also indicated that despite technological advances, the fight against terrorism was not fully utilizing the benefits of technology. The report also states that technological weaknesses in centralised information gathering and dissemination was partly responsible for the 9/11 disaster. The U.S.Intelligence Reform and Terrorism Prevention Act, 2004, was an outcome of this report and established a national intelligence program that creates and prioritises the tasks of collection, analysis, production, and dissemination of intelligence information.

To protect the nation against today's threats, it is essential that complete and accurate information is available to security agencies at the right time. Today's information management systems need to be intelligent enough to leverage the information amassed from various sources and to develop and use technologies such as data mining and other cutting edge analytical tools along with more streamlined information sharing within the intelligence community and to other relevant bodies.

Data is not considered information until it is corroborated and information is not considered intelligence until it is co-related. Today there could be scenarios where data is not considered information as the corroborative data has either not been identified or is lying with another agency and for similar reasons information may not translate to intelligence. Imagine how much this scenario could change for the better if information management and sharing tools become better integrated.

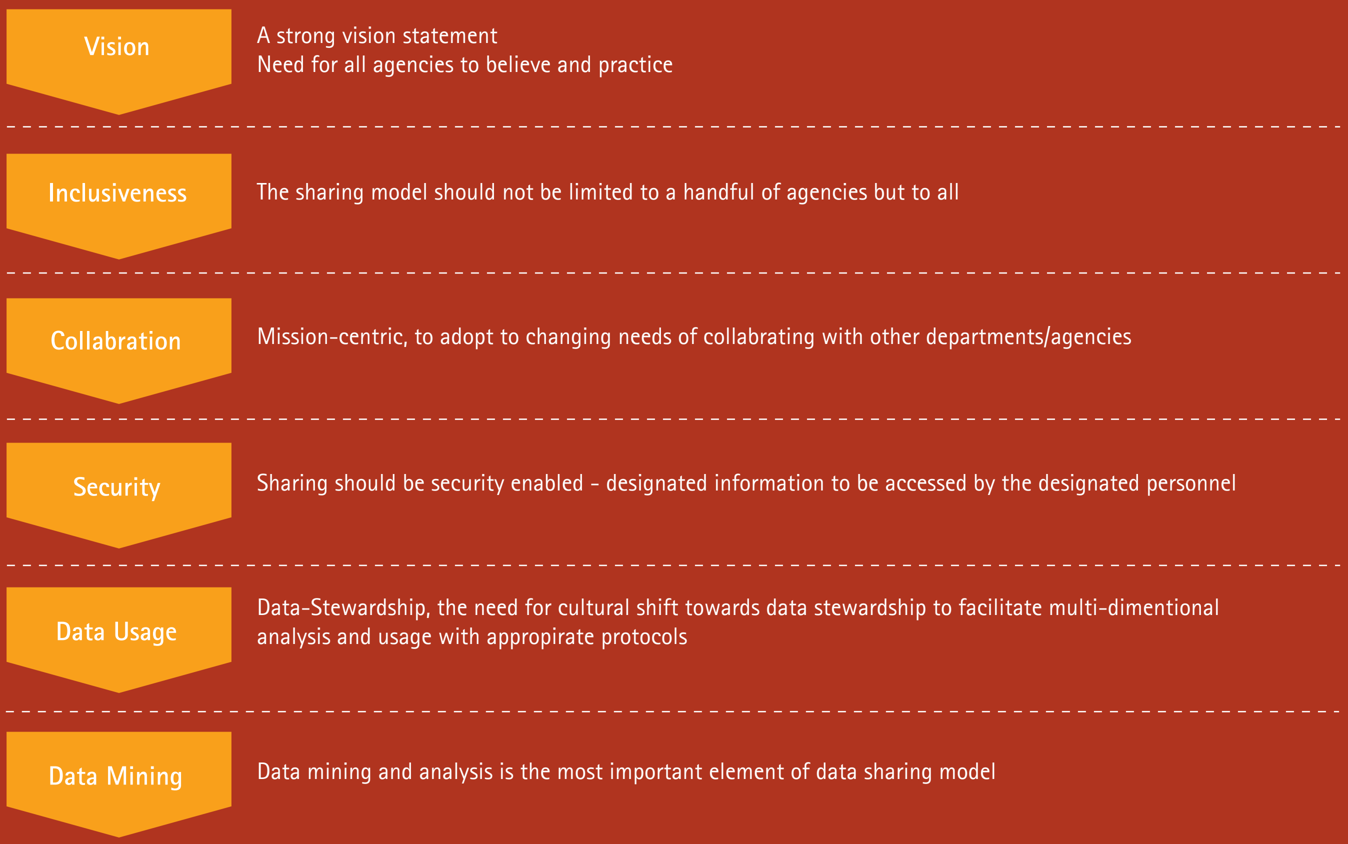
Information management encompasses the processes, functions, standards and technologies that enable high quality information to be created, stored, communicated, valued and used effectively and securely in support of an organisation's strategic goals.

The need for an information sharing model

It is essential that information is correctly and accurately classified to identify the agencies and individuals that should have access to it as well as the data handling requirements such as secure storage and safe disposal that are relevant to the content. It is also crucial that the confidentiality, integrity, authenticity and availability of the information are clearly categorised to enable the information management tool and users to handle the content appropriately.

Effective information management enables security agencies to unlock the value of information and improve their efficiency and effectiveness by:

Figure 1: Strategies of an effective information sharing model



Vision

A strong vision statement
Need for all agencies to believe and practice

Inclusiveness

The sharing model should not be limited to a handful of agencies but to all

Collaboration

Mission-centric, to adopt to changing needs of collabrating with other departments/agencies

Security

Sharing should be security enabled - designated information to be accessed by the designated personnel

Data Usage

Data-Stewardship, the need for cultural shift towards data stewardship to facilitate multi-dimentional analysis and usage with appropirate protocols

Data Mining

Data mining and analysis is the most important element of data sharing model

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

An effective and successful information sharing model is dependent on well-planned strategies. These strategies can be summarised as shown in **Figure 1.**

On December 25, 2009 there was an attempted bombing of a Northwest Airlines flight from Amsterdam to Detroit. A faulty detonator and the rapid and courageous action by passengers and crew prevented the death of 290 people on the plane and many more on the ground. The intelligence agencies had collected but then failed to piece together different threads of information about the suspect, Umar Farouk Abdulmutallab. U.S. President Obama said, "**there were bits of information available within the intelligence community that could have and should have been pieced together**" he further noted that, "**had this critical information been shared, it could have been compiled with other intelligence, and a fuller, clearer picture of the suspect would have emerged.**" This is one example of how having information management systems in place is not enough. The requirement is to have an appropriate data sharing model, backed with the power of analytics and easy-to-use data mining tools.

Addressing critical information management challenges

All internal security activities should be underpinned by robust information management to ensure the effective use of resources and data assets. However, security agencies face challenges at every stage of information management: creation, collection, storage, communication, valuation, analysis and dissemination. Unless properly addressed, these challenges reinforce data silos, inhibit collaboration and hinder data access and can prevent security agencies from unlocking the value of the information they hold and undermine improvements in efficiency and performance.

To address these challenges, security agencies must develop robust and automated information management capabilities which would involve the following:

- **Collecting information**: To reduce time spent on administrative tasks and maximise information collection, security agencies could enable remote access to enterprise information systems, ensure single-point data entry at the point of origin, digitise paper-based records and deploy effective automated data capture solutions.

- **Accessing information**: To improve the effectiveness of intelligence services, security agencies must ensure that officers can access the right information at the right time. Users must be able to access enterprise information systems remotely and locate information efficiently in highly distributed environments.

- **Sharing information**: To enable collaboration with public, private and non-governmental organisations and ensure the accuracy and completeness of information, security agencies must be able to share appropriate information effectively and securely with other organisations. Effective information sharing requires the ability to exchange data in different formats and search for data stored in external systems. Effective information sharing also requires openness to sharing information externally and a willingness to break down traditional information silos.

- **Ensuring the quality of information**: To realise the value of enterprise information systems, the information made available must be accurate and meaningful so it can be used for its intended purpose. To ensure high-quality data, security agencies must enforce common data entry standards. These standards should be supported by applications configured to encourage desirable user behaviours. 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, security agencies need effective enterprise security architectures that proactively manage security risks, effectively identify and prioritise threats, and rapidly address vulnerabilities across organisational and information silos. Data security also requires users to follow robust data handling and security policies to minimise the risk of unauthorised system or data access. Access control models and solutions must prevent unauthorised access, record access requests and assign appropriate permissions to users based on job functions.

- **Complying with legislative, regulatory and best practice guidelines**: To ensure compliance with data security, data management, auditing and operational guidelines, security agencies require a coordinated approach across organisational and information silos that enables IT, administrative and management functions to collaborate effectively. This coordinated approach minimises the cost of compliance and ensures a more effective and flexible compliance architecture.

- **Maximising the value of information**: Effective analytics solutions can improve the performance of intelligence gathering and dissemination, increase the efficiency in enforcement and administrative processes and strengthen cost-based decision-making. These solutions translate information into actionable intelligence, enabling intelligence-led and predictive law enforcement.

Internal Security Scenario and Challenges

Current scenario and future outlook

The demand for intelligence-led security has never been greater. There are a number of executive agencies and organisations that conduct intelligence activities for national security, tax evasion, money laundering and so on. These agencies include Research and Analysis Wing, Intelligence Bureau, Directorate of Revenue Intelligence, National Technical Reconnaissance Organisation, Defence Intelligence Agency (DIA), Joint Cipher Bureau, All India Radio Monitoring Service, Signals Intelligence Directorate, Aviation Research Centre, Directorate of Air Intelligence, Directorate of Navy Intelligence, Directorate General of Income Tax Intelligence, state-level intelligence organisations and others. Historically, these agencies had separate missions and lacked the capacity for coordination and collaboration but they are now being mandated to work together. Moreover, they are now required to work with other central and state-level law enforcement and crime prevention agencies in the pursuit of criminal enterprises that support terrorists.

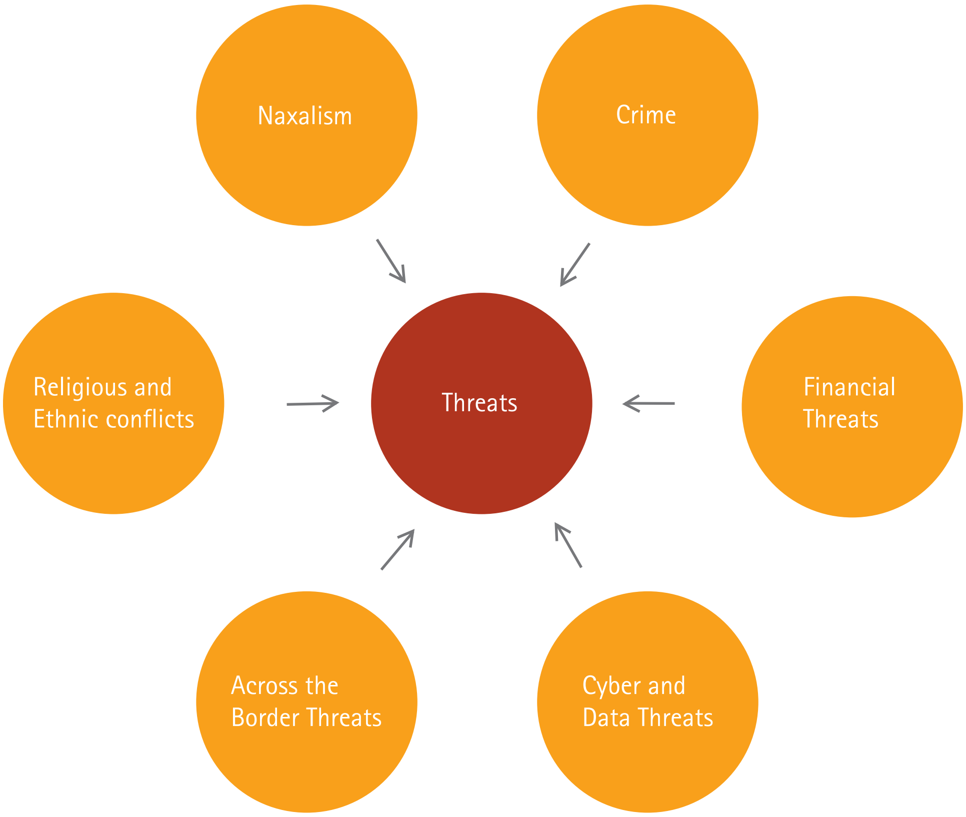
In such a large and diverse intelligence set-up with groups and agencies spread across these organisations there is a possibility that efforts will be duplicated and one might not have knowledge about another's work while pursuing the same lead, unless a robust central information sharing system is instituted. To effectively function as an efficient Intelligence structure the latest technology and expertise should be used to set up an integrated communication network.

Every day, law enforcement investigators and intelligence analysts are tasked with developing real and pursuable leads from a mountain of data. Since incomplete and imperfect data is the norm in this environment, analysts often spend valuable time on dead-end leads—never learning of essential information that might enrich a case quickly and help in a critical investigation. Imagine if investigators could quickly see how organisations, people, evidence, events and sources connected so that they could respond to and act on threats more efficiently.

Figure 2 summarises key threats India currently faces. Addressing these threats requires significant coordination across multiple ministries and execution agencies (end-users) as explained in **Figure 3.**

Image quality is good. Select Accept or Rescan
Accept
Cancel
Options
Special
Resc

Figure 2: India's Internal Security Threats

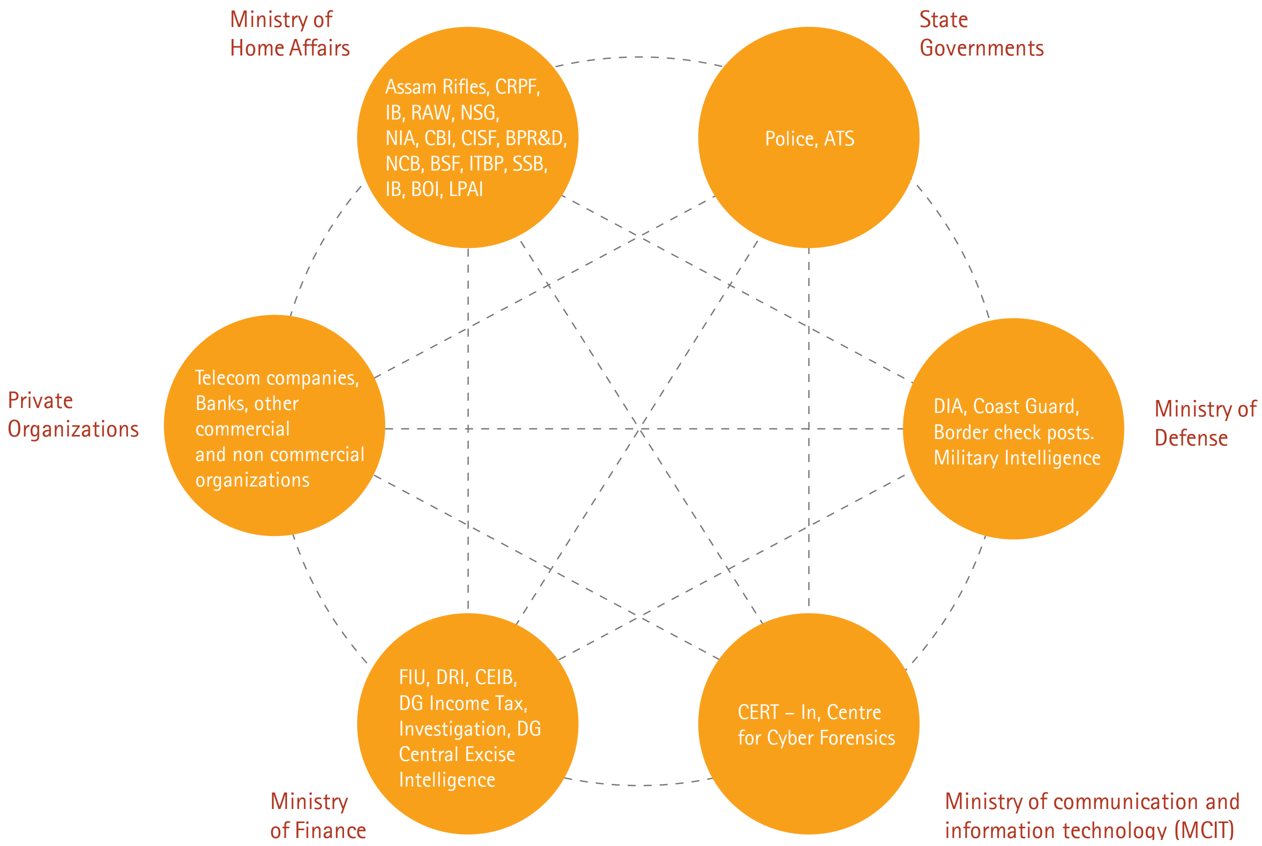


In its 2010-2011 annual report 2010-11, India's Ministry of Home Affairs emphasised the importance of information sharing and operational coordination between the central agencies and state governments to strengthen internal security. Initiatives such as the establishment of NATGRID (National Intelligence Grid), Crime and Criminal Tracking Network & Systems (CCTNS), Counterfeit Currency Information Management System (CCIMS), Talash Information System and Forensic Laboratory Information Management System (FLIMS) are the starting point to achieving a robust and connected intelligence management system.

For sophisticated application of information, there needs to be a common information management platform and a data sharing system that give access to crime information to multiple agencies and departments. The system should communicate with other systems intelligently, be able to produce intelligent analysis and enable security personnel access anywhere and at anytime within security parameters.

The vision of the Massachusetts Integrated Criminal Justice Information System (ICJIS) was to integrate traditional criminal justice and law enforcement information systems to provide each agency the information it needs, at the time it is needed, in the form that it is needed, regardless of the source and regardless of the physical location at which it is stored. The Commonwealth of Massachusetts developed an ICJIS strategic implementation plan which identified the activities and sub-projects to be undertaken by the Commonwealth to integrate its criminal justice systems together.

Figure 3: Coordination across Multiple Ministries and Execution Agencies


Ministry of Home Affairs
Assam Rifles, CRPF, IB, RAW, NSG, NIA, CBI, CISF, BPR&D, NCB, BSF, ITBP, SSB, IB, BOI, LPAI
State Governments
Police, ATS
Private Organizations
Telecom companies, Banks, other commercial and non commercial organizations
Ministry of Defense
DIA, Coast Guard, Border check posts. Military Intelligence
Ministry of Finance
FIU, DRI, CEIB, DG Income Tax, Investigation, DG Central Excise Intelligence
Ministry of communication and information technology (MCIT)
CERT – In, Centre for Cyber Forensics

Overcome challenges with a clear vision and organised information

Although information is the first line of defence against crime, sharing it is never easy. Inter-agency or cross-jurisdictional involvement can decentralise critical data, and the lack of standardised technology platforms isolates it further. However, high performance can be achieved with information-sharing strategies that garner immediate results. From intranets, shared databases and call centres to wireless technology and Web-based portals, next-generation technology can be maximised to protect citizens through strong prevention and deterrence practices.

A strong information management system should be able to prevent a devastating event and should be able to give intelligence alerts to security personnel. The coordination between agencies should be backed by a strong culture of information-sharing between central and state-level security agencies along with a robust governance system.

Better Information... Better Security

Developing effective information management - intelligent intelligence is the key

To effectively manage information, security agencies must develop workforce and process capabilities that enable efficient, effective and secure information collection, storage, use and sharing. They need to take a collaborative, strategic and enterprise-wide approach to information management.

To achieve effective information management, security agencies 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, and content management capabilities and include law enforcement, administrative and technology workstreams. Enterprise information 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 organisational boundaries.

Security agencies may implement an information-management framework (**see Figure 4**) which provides a complete model for information management and is designed to help them develop 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. This framework divides information management into five highly-interrelated disciplines and each discipline has multiple components—the most important being processes, functions and technologies required to unlock the value of information.

Figure 4: Information Management Framework

Information Management

Information Management Disciplines	Components
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 organizations 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 and procedures
	IT security
	Network integrity
	System hardening

Utilization

Security agencies have access to a huge amount of information. This information needs to be transformed into actionable intelligence to improve strategic, operational and cost-based decision-making. Analytics and visualisation tools can extract aggregated information from data and communicate information graphically to support decision-making and intelligence-led law enforcement.

To maximise the value of analytical insight, security agencies must ensure that decision-makers have timely access to relevant information at the point of need. To ensure data is utilised effectively, information management architectures must include solutions which cover:

- **Analytics** – solutions that use quantitative, statistical and exploratory analysis and predictive modelling 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 value-based decision making. Analytics can also improve the performance of security agencies by strengthening intelligence management, enabling officers to anticipate crime and supporting targeted crime prevention strategies.

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

- **Information flow optimisation** – process re-engineering programs that identify where and when information is required in law enforcement 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 security agencies by reducing the amount of time officers spend away from the field and improving their direct access to information.

Accessibility

Public security information is generally held in different systems operated by a range of organisations. These organisations include those within national security, state and central government security agencies and other law enforcement organisations. Ensuring secure and efficient access to this information requires enterprise information systems and processes that grant permissions to users based on job functions, prevent unauthorised access, locate and organise 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:

- **Access control** – role-based access control models that grant permissions to users based on job functions, and solutions that prevent unauthorised 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 organise data so organisations know where data assets are stored and can better monitor, manage, protect and access them. Effective data discovery is very important for security agencies 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 organisations.

Sharing

The growing complexity of modern law enforcement requires security agencies and other organisations to collaborate and share information more efficiently and effectively. Effective data sharing requires a sufficient level of interoperability between systems and organisations. Achieving and maintaining interoperability between systems and organisations requires common governance processes that deploy, enforce and manage interoperability standards. To ensure effective data sharing, information management architectures must include:

- **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

Germany's Federal Bureau of Criminal Investigation mandated that its 16 reporting states use its new central search system or develop a high performance technology solution to connect with it. After assessing the possibilities, the Rheinland-Pfalz Department of Police chose to develop its own system. The guiding philosophy was to keep what was good about the legacy system while taking advantage of Web-based technology. The result? An intuitive system that reflects the high performance demands of modern policing. The solution gives officers easy information access so they spend more time on the street instead of behind their desks.

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. It also requires common entomologies to ensure that concepts and relationships between these 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 organisations to use shared information to strengthen decision making and improve administrative and law enforcement processes. Process interoperability enables organisations to maximise the value of technical and data interoperability.
- **Interoperability governance** – a function that works across organisational 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 organisational silos able to share information and the level of interoperability between those silos.

Quality

Security agencies need to manage very high volumes of data from a range of sources. Ensuring the quality of that data is critical. High quality data is meaningful, accurate and 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 information systems and data sharing. As a result, it is vital that security agencies 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 components such as:

- **Data entry** – policies, training and applications that minimise 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, security agencies 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 data conforms to format, quality, integrity, accuracy and structure specifications. Enforcing common error-correction processes and data validation rules across systems and organisations 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 organisations and Standards Development Organizations (SDOs). Ensuring systems and interfaces conform to common specifications maintains data integrity 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, unauthorised access to data are critical issues for a security agency as they hold and manage high volumes of sensitive information. Data security is a priority for security agencies 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 loss of human life. Ensuring data security requires security agencies to develop policies, processes, functions and solutions that proactively manage security risks, effectively identify and prioritise threats and rapidly address vulnerabilities.

To ensure data security, information management architectures must include components such as:

- **Data security and handling policies and procedures** – policies that minimise information security risks and prevent unauthorised access to information by encouraging users to be security conscious and procedures that define how this is to be done. Effective data security and handling practices include:

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

- Minimising 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 (two factor or three factor authentication.)

- Proactively identifying and minimising security risks.

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

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

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

- **IT security assessment** – manual and automatic processes that test and evaluate the effectiveness of IT systems' information security measures. IT security assessment helps ensure that data is properly protected from unauthorised access, that all relevant security threats and vulnerabilities have been identified, and that data handling processes are correctly configured to minimise security risks. IT security assessments may be conducted by a third party and typically include a number of components including 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 prioritising 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

Incident prediction and prevention

To improve the performance and efficiency of internal security, agencies around the world are developing preventive, evidence-based law enforcement and crime prevention strategies, and focusing on intelligence-led security. 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 predictive law enforcement and crime prevention requires analytics. Analytics aggregates data from a number of different sources and uses statistical analysis and predictive modelling to identify crime trends and highlight "hidden" connections between disparate events and trends. This provides a 360 degree view of crime, enabling security agencies to predict the pattern of future criminal behaviour and identify the key causal factors of crime.

Security agencies across the US are using analytics to support intelligence led law enforcement and crime prevention to 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 law enforcement and crime prevention. 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 and crime prevention 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 law enforcement and crime prevention 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 law enforcement and crime prevention services without incurring additional cost.

Mobile data and systems access

Security agencies 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 law enforcement and crime prevention services in the United Kingdom. For example, by rolling out smart phones, Bedfordshire Police has 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 organisations 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 visualisation solutions enable officers and citizens to identify patterns and trends in crime, and security agency performance and operations by aggregating data from a variety of sources and communicating it graphically or topographically. These solutions include Graphic Information Systems (GIS), mashups that overlay crime and/or police information on interactive maps, two and three-dimensional link chart visualisations that automatically display connections between people, places, events and objects, temporal charts that highlight crime trends and crime clusters and dashboards that visualise real-time and trend performance and response data.

Operations-focused data visualisation solutions can improve the efficiency and effectiveness of law enforcement and crime prevention services by highlighting poor performance or inefficiency and strengthening evidence-based and preventive law enforcement strategies. Citizen-focused data visualisation 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 behaviour and establishing neighbourhood 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 security agencies, reduced administrative costs, improved first response and crisis management capabilities, more effective evidence-based law enforcement and crime prevention, and intelligence management.

Moreover, secure and effective information sharing enables the security agencies to develop predictive analytics and data visualisation solutions that are critical to intelligence-led law enforcement and crime prevention. To achieve these benefits, security agencies around the world are establishing state, regional and national information networks that enable secure and effective information sharing between numerous law enforcement and public safety organisations.

Some U.S. 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 realising 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 organisation, facilitates cross border police cooperation in part by providing security agencies with an infrastructure that enables them to share information internationally. Interpol provides all its member countries with instant, direct access to a 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 security agencies and other organisations 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 organisations. It is achieving this through a number of programs that promote and enable interoperability between disparate systems and organisations at local, state and national levels:

- **Fusion centres and intelligence sharing** – fusion centres bring together all relevant public safety, law enforcement and private organisations involved in preventing and responding to criminal and terrorist activities. Fusion centres provide "effective and efficient mechanisms to exchange information and intelligence, maximise resources, streamline operations, and improve the ability to fight crime and terrorism by analysing data from a variety of sources." To achieve technical, data and process interoperability between different organisations, fusion centres focus on designing and embedding "processes through which information is collected, integrated, evaluated, analysed, and disseminated." Working with a 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 centres and achieve a high level of interoperability between systems and organisations. 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 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 technical and data interoperability by providing a standardised 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. 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.

o Providing technical tools to support development, discovery, dissemination and re-use of exchange documents.

o Providing training, technical assistance and implementation support services for enterprise-wide information exchange.

Way Forward

Any breach of internal security, apart from the possible loss of human life, impacts the image of a nation. It is of utmost importance that internal security agencies are equipped with policies and technology to be able to predict, prevent and act on any impending threat to the nation. There is no doubt on the role played by information in the security world and how critical it is for the right information to be provided to the right people at the right time. With advances in technology and sophisticated tools, information is being collated, analysed and shared in a much more efficient and effective manner and at pace.

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

The critical first step in designing and deploying 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 organisational 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 organisation's strategic goals. Adopting a comprehensive, structured approach to information management, such as the information management framework for internal security management (see Figure 4), will help ensure security agencies develop effective information strategies that improve the efficiency and performance of their services.

Based on our research, we have defined a set of best practices for internal security agencies developing an **information strategy**:

- **Involve a range of stakeholders -** An effective information strategy will cut across organisational silos and will impact operational, technology and strategic functions. Information strategies should be developed and refined through a collaborative process that brings together perspectives from a range of functions including frontline 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 organisation, 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, 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 organisation's information strategy should explicitly link with its strategic priorities.

• **Do not neglect the cultural and organisational dimensions of information management** - Improving the effectiveness of information management requires cultural and organisational change and new information systems. There are three main cultural and organisational dimensions to information management that should form part of an organisation's information strategy:

- **Training and education**: ensuring that users understand how to use IT systems effectively to improve – efficiency and performance.

- **Operational processes**: redesigning operational processes to maximise 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 treats information as a valuable strategic asset.

• **Analyse the latest technologies** – It is highly pertinent to look at existing mature and stable technologies as well as considering the latest and emerging technologies. The right information strategy is always a good mix of existing and emerging technologies. The existing technologies provide the stability and strength to predict, prevent and act on potential threats and emerging technologies provide the nation the capability to stay ahead of the curve.

Some of the key takeaways from our research are:

a. Review the way policies are structured. Are they effective, efficient and provide security agencies the agility to act fast and firmly on people who intend harm to our internal security.

b. Create an information strategy including IT strategy for each agency, which will provide the ability to collate, analyse and share data in an effective and efficient manner.

c. Strengthen agencies with the right tools and technologies available.

d. Incorporate change management to encourage information sharing and improve the quality and completeness of information

Information is at the heart of modern day internal security, law enforcement and crime prevention and detection and security agencies have to rely upon effective information management. As a result, strengthening information management is critical to increasing the efficiency and effectiveness of security agencies. Improvements in information management will drive and support improvements across the board by providing security agencies with timely access to high-quality, accurate, relevant and holistic information that strengthens decision-making and improves operational performance.

References

- NATGRID Project Gets in Principle Approval – NATGRID (National Intelligence Grid), http://pib.nic.in/newsite/erelease.aspx?relid=72527

- Chief Ministers' Conference on Internal Security to be Held Tomorrow – discusses Crime and Criminal Tracking Network & Systems (CCTNS); http://pib.nic.in/newsite/erelease.aspx?relid=69443

- Spiralling fake notes strike note of alarm – discusses Counterfeit Currency Information Management System (CCIMS); http://www.dailypioneer.com/205481/Spiralling-fake-notes-strike-note-of-alarm.html

- http://www.dfs.gov.in/Tenders/lims.pdf - discusses Forensic Laboratory Information Management System (FLIMS)

- Major Achievements of MHA since December 2008 & Report Card for May,2011, http://pib.nic.in/newsite/erelease.aspx?relid=72445

- India-US Homeland Security Dialogue Concludes. Two Sides Affirm Strategic Importance of Mutual Cooperation in Tackling Terror & Other Security Issues; http://pib.nic.in/newsite/erelease.aspx?relid=72365

- "Accenture Border Management and Public Safety - Protecting Public Safety" published by Accenture; http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Protecting_Public_Safety.pdf

- "Information Management in Policing Improving efficiency and performance by unlocking the value of information" published by Accenture Institute for Health & Public Services Value; http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Information_Management_in_Policing.pdf

- Annual Report 2010-11, Ministry of Home Affairs, Government of India

- United States Intelligence Community, Information Sharing Strategy, February 2008; http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf

- http://www.fas.org/irp/congress/2006_rpt/hsc-dem.pdf

- Factiva Newsstand," It was a catastrophic breach of security: Obama " 30 December 2009, Indo-Asian News Service

Contacts

Adarsh Parekh
Health & Public Services, Accenture
adarsh.parekh@accenture.com

Authors

Krishna Giri, Managing Partner, Health & Public Services, Accenture India

Adarsh Parekh, Lead – Identity, Border Management and Public Safety, Health & Public Services, Accenture India

Maneesh Chandra, Lead – Security, Technology Consulting, Accenture India

Pradeep Roy, Senior Manager, Accenture India

Hema Santosh, Manager, Accenture India

Anurag Johri, Manager, Accenture India

Rajat Garg, Manager, Accenture India

Disclaimer

This Report has been published for information and illustrative purposes only and is not intended to serve as advice of any nature whatsoever. The information contained and the references made in this Report are in good faith, neither Accenture nor any its directors, agents or employees give any warranty of accuracy nor accepts any liability as a result of reliance upon the information, advice, statement or opinion contained in this Report. This Report also contains certain information available in public domain, created and maintained by private and public organizations. Accenture does not control or guarantee the accuracy, relevance, timelines or completeness of such information. This Report constitutes a view as on the date of publication and is subject to change. Accenture does not warrant or solicit any kind of act or omission based on this Report.

About CII

CII Defence, Aerospace and Security Initiative

CII Defence, Aerospace and Security Division works under the guidances of the CII National Defence Council (erstwhile CII National Defence and Aerospace Committee). It has a mandate to implement and promote Confederation of Indian Industry's (CII) initiative for Defence, Aerospace and Internal Security.

The Committee (now council) was formed in 1993 and has been proactively working with the Ministry of Defence, Ministry of Home Affairs, Armed Forces, DRDO, Defence PSU's, Ordnance Factory Board, various security agencies and the private sector. The objective of this council is to "Establish a strong partnership between Defence and Security Services & Industry and enlarge the role and scope of Indian Industry in Defence Production & Supplies for mutual benefit and enhance the National Security". The Council strives to forge industry initiatives to strengthen the Indian Defence Sector.

The Government has allowed 26% FDI in Defence Sector. Also, the Ministry of Defence has recently announced a revised Defence Offset Policy in Defence Procurement which is also extended to aerospace and internal security sector. It is perceived as an opportunity for various countries to establish JV and Technological Collaboration with the Indian Industry to set up production facilities in India. To encourage, TOT (Transfer of Technology) and Joint Ventures, the CII Defence Committee regularly takes Defence Industry Missions abroad.

The Defence Council has been active in creating international linkages. In this regard the council had worked very closely with the US Industry to promote India-US Industry Co-operation in Defence & Strategic trade. Similarly, Besides, CII has MoUs with several international business organisations.

With the backing of CII's wide national and international network, CII National Defence Council serves as a reference point for Indian Defence Forces, Indian Defence Industry and the International Business Community.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 223,000 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.

11-1217_af / 02-2701