

white paper

Interoperability — The Best Way to Leverage Information for a Secure Community

Gerry Wethington

reliability

Analyzing existing data in unconventional ways can improve government's day-to-day operations and coordinated response.

Introduction

For timely response to justice and public safety events, dependable communication is critical — and government agencies must deliver the right information at the right time to the right people for effective decision-making. However, it is important to understand the distinction between data and information. Data is seldom actionable, since the content itself has not been analyzed through any particular business process lens. The business process lens is essential, because data viewed through a first responder lens may not have the same value to a government public works director. It is in applying the business process analytics to data — that actionable information is created and value generated.

A good example is the data generated by a typical 311 contact center. In addition to directly improving citizen services, through more efficient handling of non-emergency calls, a 311 contact center can also provide additional information for business intelligence in justice and public safety agencies. Information gleaned from 311 contacts that has an impact on justice and public safety could be routed as appropriate to law enforcement, providing another data stream to analyze. In addition to 311 data, other sources could be synthesized as well — such as information from police on the street sent via the computer aided dispatch (CAD) system — and analyzed to assess the magnitude of an event.

And with public safety's increased emphasis on joint operations and task forces in light of the recent hurricane-related disasters that demonstrated the need for multi-jurisdictional response, the requirements for interaction among users of information has increased exponentially. At the same time, the potential sources of information — traditional computer-generated data, email text, voice, images — have never been more voluminous. And with shrinking budgets, state and local governments face numerous challenges as they attempt to develop interoperable systems to get that information to those who need it.

This white paper presents some relevant examples of creating actionable information from data to support key public safety business processes. It points out that in most cases the data is coming from multiple organizations,

through multiple systems and in multiple media, which makes interoperability essential. While technology is no longer an obstacle to interoperability, the policies and culture of organizations can still inhibit information sharing. The white paper concludes with some recommended techniques for improving the visibility of information across different organizations and systems to achieve a more secure community for our citizens.

Creating Actionable Information from Data

Consider the emergence of 311 systems. With their introduction, governments have opened up a new citizen communication channel with the potential to be a rich source of information, particularly if business analytics are applied. Government traditionally responds to the requests put forth by the citizen through action taken by the call taker — who either answers the question, routes the call, or assigns a task to a responsible department.

The value of a 311 contact centers has already been well-established. Typically where a 311 system is implemented, non-emergency 911 calls have been drastically reduced, allowing emergency dispatchers more time to respond even more quickly to true emergency events. But the value of the information doesn't have to end there. What if the content of the 311 call were digitized and analyzed over time to identify patterns and trends? The resulting content would most likely produce information that would allow government to evaluate programs, service offerings and resource allocations to achieve maximum service levels and operational efficiencies. This represents a capability not prevalent today; instead, call characteristics and patterns are spread across multiple call-takers, and pattern identification is limited to their personal call exposure and their ability to remember prior calls. If the data were instead digitized and then transformed into actionable information by applying analytical software, such as pattern recognition, would we look at programs differently? Would we better understand consumer expectations and demands?

As in this 311 example, the process of transforming data into actionable information often requires combining different types of source data. For some sources, like voice,

this process first requires that the source data be digitized. The digitalization of data is not uncommon. We encounter it frequently, but probably don't recognize it. When was the last time you made a phone call and were asked by an automated voice response system to provide your account number, frequent flyer number, catalog number or package tracking number? Voice recognition software then converts that to digitized data that can be associated with other data sources, such as your computer record in a customer relationship management (CRM) system — the private sector equivalent of a 311 contact center. These are all common business practices in the private sector that are making their way into the public sector, most notably in the benefits distribution space. In the public safety space, digitizing voice data in support of a secure community has tremendous potential.

The process of digitizing voice source data for building actionable information is being simplified with the emergence of Voice over Internet Protocol (VoIP) technology. With VoIP, voice source data is effectively already digitized. VoIP involves digitizing voice and transmitting it over a broadband Internet connection instead of traditional analog telephone lines. It has received significant attention in recent years as a cost-effective option for telephony, but other benefits include unified messaging, which effectively combines voice and text data sources. Microsoft and Google, for example, have obviously seen the future and are each pursuing VoIP strategies, with Microsoft purchasing Teleo, a VoIP software and service provider, and Google introducing its Google Talk instant messaging and VoIP service.

The growth of VoIP shows that voice communication has evolved into another form of digitized data. This convergence underway of voice and more traditional forms of data has made it possible for justice and public safety agencies to have even greater access to information. The technology infrastructure is no longer the major barrier to assembling data from multiple sources or sharing information with multiple users. Increasingly, it's all just bits through the same Internet Protocol (IP) pipe. The problem is no longer with the choice of pipe (IP is a well-established transport standard), and is less and less with the bandwidth of the pipe. Rather, the question that remains is: What do we do with all of that input?

Consider the old Management Information Systems (MIS) approach to utilizing reporting by exception. In the late 70s and early 80s when MIS systems, such as the federally-mandated State Medicaid Management Information System (MMIS) standard, were the rage, government was already drowning in information. MIS was an attempt to manage the volumes of data. What was missing was the application of metrics and threshold management principles. The most effective way to manage the volumes of data that exist is to understand what metrics you are trying to achieve. Government is starting to recognize the value of not only **outputs**, but more importantly, **outcomes**.

As government accepts and implements metrics programs, such as the U.S. Federal Government's Balanced Scorecard, with a focus on outcomes, it can begin to identify the thresholds within which they are willing to operate. When those thresholds are applied to the volume of data, government can then focus on that information that falls outside the areas of acceptable public safety, acceptable service delivery, and so forth. Additionally, government can focus on those programs that are achieving the desired outcomes. And by managing the artifacts associated with program or service delivery excellence, government can begin to replicate those patterns throughout the enterprise.

An Issue of Policy, Not Technology

Government jurisdictions are taking steps to allow information exchange across agencies and jurisdictions — even beyond the justice and public safety realm. Further, the analytics capabilities long used in the private sector, which are now available to government, mean that the lofty goal of accessing genuinely insightful information is finally within reach.

But accomplishing the requisite interoperability among government agencies and their systems is no easy task. In voice communications, disparate frequencies and radio technology, the deterioration of existing systems, low funding levels, as well as the competition for spectrum resources, pose considerable challenge to public safety agencies seeking interoperable solutions.

The biggest challenge, however, is no longer the technology. Rather, the challenges come from agencies clinging to outdated policies and the reluctance of appropriation bodies

to fund infrastructure upgrades that will support interoperability standards, such as extensible markup language (XML). And the fear on the part of administrators of losing control of their environment if they embrace interoperability solutions.

The reluctance to embrace new technologies — and more importantly, new operational practices — is somewhat understandable. The public sector has spent more than 30 years investing in technology silos and most governments today have a complex and confusing mix of legacy hardware, operating systems and application development environments that cannot easily be replaced. Adding new technologies only adds to the complexity and confusion. But, even where investments have been made in common technology platforms, often in central data centers, the responsibility for the applications that run on those common platforms almost always rests with the individual user agencies. That's where the reluctance to look at common business processes across agencies and embrace new operational practices helps keep the silos intact.

An element that must be introduced and seriously considered by those with administration responsibilities is not the loss of control. Rather, it is what transformational improvement could be accomplished in public safety, public service and responding to latent demand — if instead of staking claim over everything they were able to deliver, they focused on what they are uniquely qualified to deliver. The concept of commodity utilization has to be considered in making policy changes. Administrators must also consider the time factor in the distribution of information. Building multiple layers of ownership, control, distribution and utilization serves to only extend the timeline for information dissemination.

Given the technology capabilities today of interoperability, infrastructure outsourcing and even infrastructure insourcing, the factor of timely dissemination of information can be overcome. With a real focus on the timely delivery of information, and the setting aside of the traditional ownership and turf issues, lives can be saved — among law enforcement, first responders and citizens. It truly is about getting the right information to the right people at the right time. The last requirement of that axiom is extremely

time sensitive and requires a fresh look at what have become traditional responsibilities and traditional process and data ownership.

But interoperability is critical for delivering services to the public, according to the National Association of State Chief Information Officers (NASCIO) assessment of interoperability and integration in the United States. Today's cooperative efforts require voice and data communication — despite the fact that public safety and public service still have technical and cultural problems with interoperability¹.

While the exchange of justice and public safety data is critical during a crisis, it is also important for the day-to-day administration of government business. Information interoperability involves more than just voice, data and pictures; this is a case in which the whole is truly greater than the sum of its parts, and achieving the requisite wholeness involves analyzing the existing sources to provide a richer form of insightful information, delivered seamlessly over multiple channels.

This new **information interoperability** will become possible through the acceptance of industry-wide standards, such as XML. It also requires the application of business intelligence techniques to enable governments to make meaningful connections, glean powerful insight, and foster a new way of thinking about data and its implications for securing the community. In all, it foretells a major cultural shift in the public sector.

Information Sharing through Timely Data Exchange

Increasingly, states have recognized that interoperability among various systems is imperative to achieve the inter-agency information interoperability that they require to adequately protect and serve their communities. While there has been much recent attention on voice interoperability for first responders, the need is no less critical as it relates to interoperability between computer data-oriented systems, such as computer-aided dispatch (CAD) and public safety records management systems (RMS).

One needs to recognize that time and lives are not saved just through inter-agency collaboration. Intra-agency

interoperability is equally important, if not more so. What if an agency could save time by ensuring that when a record is entered into an accident system that the entry is first checked against the citation system, the warning system, and the calls-for-services system to ensure that contact information is not duplicated but rather reused? Those additional checks would result in better, more accurate and more timely information. They would reduce data entry efforts. And embrace the integration principles of capturing data as close to the source as possible, entering data once and reusing it many times. Public sector resources would be more effectively utilized, latent demand reduced, data quality improved, and public safety and the public better served.

But increasingly, for either type of sharing, many state and local governments are restricted by budgetary constraints, legislative barriers, turf battles and cultural issues that must be resolved.

Rather than offering every participant an open-access pass to all information — which could potentially compromise the privacy of individuals — state and local governments must selectively push data to subscribers. Determined by the business rules that are extracted from existing or new business processes that describe their operations, these information exchange activities must reflect the needs of each participating agency, taking into account the conditions under which each recipient needs or wants information.

It's important to note the information technology confidence factor. Consider the technology that the majority of public sector administrators first encountered when their manual data systems were automated. The technology wasn't capable of data attribute-level security, biometric recognition for security access, publish or subscribe features — just to name a few recent advances. Most administrators' first impressions of security capabilities are based upon entire system lock-down features and, at most, entire database restriction capabilities.

Today's technology has matured significantly; unfortunately, it is still being held accountable to those earliest impressions of security capabilities, which established that first impression of information security and privacy confidence factors. We each have an obligation to educate

ourselves on the maturation of technology security, privacy and timeliness capabilities. It's important to understand that the business rules must facilitate faster access to relevant information — ideally in real time.

Maintaining a secure community today requires the real-time exchange of pertinent information, and to achieve this, public sector agencies must break out of a very traditional mindset, and instead use information in entirely new ways. Agency systems must be constructed or adapted to deliver information into the hands of people who need it to act preventively. And at the same time, fulfill the expectations of today's constituents.

The key is delivering powerful, actionable information — much more than just data — to the people who are charged with securing the community at the state and local level.

Untapped Potential

Interoperability — the real-time sharing of that information across multiple systems — is critical for the efficient day-to-day operation of justice and public safety agencies. It's also the foundation of coordinated response by police and fire departments, healthcare providers, transportation officials and military support during multi-jurisdictional emergencies.

To access the untapped potential, it is extremely important to recognize the role of architecture and standards in our planning. Architecture provides the basic blueprint of what we need — on four different levels: organizational strategy, business process, software applications and IT and communications infrastructure — to exchange information with another entity.

Standards provide the rules of engagement in how we employ that blueprint in the data exchange environment. Within the architecture space, many organizations — including NASCIO, the Office of Management and Budget, and Global (the Global Justice Information Sharing Initiative) — have established the value of architecture for public sector organizations and provided guidance on the implementation of this discipline. Within the standards area, the Global Justice XML Data Dictionary (GJXMDD) has set the standard that is rapidly being adopted by government

agencies on a global scale. It is the rigor of architecture and the value of standards that offer the best opportunity to realize the untapped potential offered in achieving interoperability. With an architecture blueprint built to standards agreed to by participating agencies, data can be exchanged in a manner that allows sending agencies to effectively communicate what they're sending, and helps receiving agencies accurately interpret what they're receiving.

Although many see the value in and are moving toward greater interoperability in government agencies, few jurisdictions possess truly integrated capabilities in which data from multiple agencies is exchanged in real time when and where it's needed. That's nowhere more the case than in the justice enterprise, and in what is typically called "integrated justice," in which the handoff can be done automatically through a single query, without manual (or human) intervention of any kind. In a recent Unisys telephone survey of 70 justice jurisdictions in the U.S. and selected foreign countries (including Canada), fewer than half (43%) reported they could access multiple databases with a single query. In fact, among justice professionals surveyed in a subset of these respondents, "obtaining all information regarding a person/case from a single query" was among the top three preferences in an integrated justice information sharing system.

What's needed now is a new way of viewing data and its potential, regardless of delivery channel — whether computer, radio, mobile phone, PDA, or other means. State and local public safety departments can't afford to cling to old values and methods. And from what we've seen during our work with state and local government agencies, the wholesale replacement of existing systems with new ones is unrealistic in today's budgetary environment. Instead, it requires leveraging existing systems to identify valuable information.

Unisys has implemented this four layer approach with our 3D Visible Enterprise methodology, which makes clear how every layer of business affects the others.

Strategy: *Where business vision and operations meet, value improvement opportunities are identified, objectives are determined and key performance indicators are set.*

Process: *Where vision is carried into information sharing across every segment of the justice value chain — from law enforcement investigation and arrest to correctional system incarceration and release*

Applications: *Where business processes are translated into a complete Blueprint solution*

Infrastructure: *where the foundation of a visible, agile justice enterprise is scalable, reliable and expandable to meet your needs.*

As we've emphasized in this paper, interoperability can't be considered only at the Infrastructure and Applications layers if we want to be able to create actionable information from data. Information is actionable only when it relates to the receiving organization's strategy, mission and objectives and can be interpreted in the context of the organization's business processes.

Based on proven process models and reusable code, 3D Blueprinting allows you to replicate successes across functional lines, and to share them with other agencies and jurisdictions. With 3D Visible Enterprise you can model the impact of change and investments before you make them. With visibility into key information sharing processes, you can protect your enterprise, data, personnel and citizens against:

- *Poor decision-making and unnecessary delays in the criminal justice process because of incomplete information, and*
 - *Threats to staff safety and domestic security because individuals aren't identified accurately and quickly*
 - *And you can maximize value by linking with legacy systems, instead of replacing them.*
-

Valuable Data Relationships

All of us involved in the systems and solutions used in the administration of government at large, and of justice and public safety in particular, need to take a fresh look at available data sources, including voice and image data, to identify and leverage their untapped potential. In this way, government can obtain new information from its traditional data sources, building the foundation for enterprise-wide information interoperability.

How? By documenting, modeling and adapting business processes. In addition to ensuring, for example, that multiple radio systems can interact to share timely information when needed, achieving information interoperability involves extending the value of information by examining the value of data relationships beyond traditional public safety users to the broader community of responders to any disaster or incident. That means we must reach out to new or underserved stakeholders such as hospitals, mass transit workers, schools, agriculture, natural resources, financial markets and public utilities.

The increased interest in interoperability echoes interest among public and private sector officials in the efficient and effective delivery of services, whether those services involve public safety or commerce. In our experience with public and private sector organizations seeking to improve visibility and security of people, business processes and information, we've found that proven, enterprise-scale solutions can also reduce costs and increase efficiencies.

Efficiency that Increases Safety

Interoperability provides significant downstream value to public sector agencies — specifically, public safety — where it can help redirect staff resources. That is, it satisfies “latent demand” for services, freeing up a community’s dispatch staff to do what they are uniquely qualified to do. Or to accomplish tasks they didn’t have time to do address previously, but that are important and either improve services, or increase the safety of the community. All while providing information to law enforcement officers more quickly.

For example, if a state deploys a wireless notebook system for law enforcement officers in the field, dispatchers won’t have to spend significant time answering routine inquiries from officers in the field — instead, those officers can query multiple databases themselves, gaining direct access to the information they need without having to work through another organizational layer that could slow down the process or introduce error. Dispatchers can instead address inquiries involving interagency cooperation and collaboration, or capture and begin cataloging business intelligence or business process information, or conduct further analysis on existing data to identify patterns that provide additional insight to law enforcement.

Information interoperability also increases speed of response times. For law enforcement officers who are interacting with the public in tense situations, faster response times can literally mean the difference between life and death.

Moving to such non-traditional uses of data provides still other benefits. As an example, for a Registered Traveler Pilot program at three major airports, Unisys verified the identity and assisted the government in assessing the suitability of program applicants. This risk assessment included a voluntary passenger background check. The data was used in an unconventional way, with the emphasis on identifying people who didn’t pose a threat to security, rather than weeding out those who posed a higher risk. This was a distinctly different use of background check data that required a change in traditional attitudes about justice and other data.

Once enrolled in the Registered Traveler program, frequent fliers are able to move through security checkpoints faster using a secure smartcard and biometrics. The program streamlines passenger processing by effectively giving airport screeners more actionable information on these travelers. In addition to reducing the amount of time registered travelers need to spend at the airport, it has the secondary benefit of reducing the number of passengers in the airport screening area at any given time, so law enforcement would have fewer people to deal with in the event of an emergency.

Business Rules Development

An initial challenge comes from identifying the business processes that facilitate the exchange or use of information — that is, the conditions under which information will be shared, with whom and when — and establishing business rules that capture those conditions.

Identifying and cataloging business rules provides several benefits for the organization. It gives agencies an opportunity to document their business continuity and disaster recovery plans, while identifying their business flows. And, because it is estimated that 30 percent of state workers will be eligible to retire² by 2006, it protects the organization from a rapidly shrinking workforce by capturing the institutional capital in the form of business rules and use cases.

Analyzing the sources of the information that agencies rely on today provides insight that could be applied to the development and implementation of a state's information interoperability framework.

The Justice Information Exchange Model (JIEM) tool, developed by SEARCH, the National Consortium for Justice Research and Statistics, is a good example of how this can help the justice and public safety enterprise. JIEM is used to capture information exchanges in the justice arena. It also holds promise for capturing information exchanges and identifying areas of overlap within other areas of government.

Similarly, law enforcement's 10-Codes, which govern radio-based information exchange between responders, could be a rich source of information to help determine what additional information exchanges they might need. Knowledge about the frequency and circumstances of use of these codes, and the types of additional information users need in order to respond to an incident, usually exists today only as anecdotal information inside the heads of radio dispatchers. However, data on the usage of these codes could be analyzed to provide insight into the agency users, triggering events, information requirements and conditions (in JIEM terminology) needed to define use cases and business rules for an interoperable system that would provide all the right information to responders when they need it. This information might be sent, for example, via cell

phone or mobile data terminal directly to the responder as a follow-up to the radio message.

Addressing business architecture issues requires government entities to consider inter-agency distribution of data, determine the business rules and decide how information will flow. Modeling can also illustrate the impact of the solution on the entire organization, as it provides information to and receives information from outside organizations.

Analytics that Change Behavior

Traditional applications and data are now being extended through the application of non-traditional methods, and the accelerating convergence of data and voice in support of interoperability. Just as business intelligence is used to analyze today's consumer spending habits — where a credit card company might prompt a business to confirm a card user's identity, or notify a customer regarding possible identity theft as a result of unusual purchase patterns or locations — business intelligence could also foster a predictive approach to public safety and security.

By using analytics to look at data structures and data values, to compare content to business situations, and identify patterns, justice and public safety agencies can use analytics to explore data relationships to determine their usefulness and value in achieving an agency's stated goals. As patterns are identified, predictive analytics can then be applied so that public safety agencies can apply them to detection and prevention activities. This information must be routed to the appropriate personnel, ideally in real-time, to avert disaster.

Analyzing a community's data can enable law enforcement to determine what is relevant — or, what's actionable — and then begin to influence the behavior of law enforcement as well as citizens. That final step, involving behavioral change among the public sector service provider, is critical for achieving a secure community.

By comparing patterns of data to traditional and non-traditional events, public safety agencies can take a proactive approach to protecting the community. This technology is slowly making its way into the public sector in public safety and benefits administration, as well as service delivery, education, transportation and regulatory programs.

For example, traffic citations, warnings and accident reports are seldom mapped against the geographic location of schools and daycare centers, and the names of violators within certain geographies aren't always compared to sex offender registries. If they were, preventive action via stepped-up patrols could be taken when the data shows a

connection — a clear example of how applying business intelligence principles to the data can result in what might be termed “full interoperability,” and improved public safety. The chart below, *Information in Action: Chemical Leak*, demonstrates how this concept of full interoperability also applies to non-traditional public safety incidents.

Information in Action: Chemical Leak		
A chemical plant has a small temporary leak that is corrected. However, the drift, albeit small, can be deadly. A highly dangerous plume from the leak is moving toward a major thoroughfare. The chemical plant must get this information to the transportation department and law enforcement for traffic rerouting within the next 10 minutes, because the drift could kill people caught in its path over the next 15 minutes, until the drift dissipates to an acceptable parts-per-million level of air saturation.		
	Event	Results
Limited Interoperability	<ul style="list-style-type: none"> Hospitals are alerted about potential casualties by the dispatcher although this requires a public safety / health care industry relationship that may or may not exist. Police drive through neighborhoods, urging citizens via loudspeaker to evacuate due to the danger posed by the drift. Police set up traffic detours to reroute or possibly stop traffic from entering drift area. This requires timely notification and available officer to execute the plan. It does not leverage the factor of an informed public. 	<ul style="list-style-type: none"> Delays in informing the general public increase the number of citizens who are at risk of injury or death.
Full Interoperability	<ul style="list-style-type: none"> Automated calling trees that are structured based on a particular disaster scenario are used to notify the proper emergency management authorities. A PC-activated radio communication is sent out to officers in the area, as determined by a GPS plotted traffic map, updated in real-time. Hospitals are alerted at the first sign of a crisis, depending on geographic location of the spill (as determined via GPS capability). E-mails are sent to those citizens and stakeholders, such as local hospitals, who subscribe to event-notification services. Citizens are contacted via home phone, cell phones, and PDA based upon their subscriptions and order of contact preference. Mass-transit systems are engaged to assist law enforcement in evacuating residents, freeing up police and hazardous materials teams to manage higher-level public safety aspects of the disaster. Automated highway signs are updated to inform motorists. Citizens are quickly informed and evacuated. Mass-transit bus system is used to evacuate people in the neighborhood adjacent to the spill to safety. Hospitals are better prepared to quickly deal with the emergency. 	<ul style="list-style-type: none"> Citizens are quickly informed and evacuated. Mass-transit bus system is used to evacuate people in the neighborhood adjacent to the spill to safety. Hospitals are better prepared to quickly deal with the emergency. Fewer casualties result.

Authentication and Access Management

Ensuring that a justice and public safety's business operations maintain security, trust, reliability and privacy is paramount — and controlling access to sensitive and private information begins “at home.” Cross-agency sharing of information raises user authentication and access management concerns. These concerns were echoed in research conducted by Unisys during the 2004 SEARCH Symposium on Integrated Justice, during which survey respondents were asked to rank 10 features of an integrated justice information sharing system — and User Authentication/Access Management emerged clearly as the most popular feature among respondents.

Confirming a user's identity and access rights enables the protection of strategic assets — such as access to justice and other government information, as well as its processes and systems — thereby reducing vulnerability and keeping exposure to a minimum through the complete awareness of both internal and external dependencies.

The Visibility Age

Adopting an information interoperability approach makes training all the more critical, since it likely involves updates to a state's business processes or workflows, as well as greater involvement in data interpretation. Staff needs to understand how their ability to access additional data will affect operations.

Perhaps equally important is a common understanding of how information will not be used. For example, after a Radio Frequency Identification (RFID) tracking system was instituted to identify inmates and guards in real time, some correctional officers at Calipatria State Prison in California were initially opposed to the idea, fearing they would be tracked and their whereabouts used against them. But the prison agreed not to use the data against the officers, who now support the system.

RFID has also been used tags in police patrol cars in various jurisdictions, and although initially the tags were thought of as intrusive and invading privacy, officers have come to see that there was a benefit: the tags aren't used to track them personally, but to help them do their jobs better. By tracking their location using a combination of RFID and GPS systems, police officers engaged in car chases can receive updates about roadblocks ahead or dangerous intersections.

Training on enterprise-wide information interoperability must remain focused on learning new business processes, with less emphasis on the new technology itself. Today's government workers need additional training on new and emerging business models, as well as new economic models and process models that can affect how they do business.

Agency personnel must learn exactly what new information is available and how it will be delivered. They also need to understand and incorporate into the workflow any new business practices or processes that may be necessary to facilitate information sharing. Staff must also understand the behavioral changes that are necessary to take best advantage of the new information they'll receive.

Unisys has seen that modeling business processes, in particular, can help government agencies see the impact of new solutions and systems — or even a change in those business processes — on their entire organization. By modeling their business processes and their underlying systems, the result is increased visibility — the ability to see the impact of information and resource sharing across the enterprise.

A state can first create models of its existing business processes, information captures and exchanges, and then document the ideal “to be” state — by documenting the new business rules and system actions that allow law enforcement and homeland security personnel to share voice, data or image information. After discovering the linkages between an organization's processes, applications and IT systems, the impact of future activities becomes easier to predict, manage and plan. Making risk easier to manage.

By comparing the current environment to the state's ideal interoperable environment, the points of interest — where the interoperability could add value to the current environment — become clearly visible. This methodology has been used successfully by Unisys in a wide range of interoperability environments, and is consistent with the Enterprise Architecture model endorsed by NASCIO, which is being adopted by many states.

Summary

Today's government is no longer constrained by technology; instead, the technology exists to accomplish virtually anything with the data sources at our disposal. And based on their experiences with technology in the commercial sector, the public's expectations of technology in government have greatly increased over the past decade and will continue to drive development of new systems for service delivery.

Local justice agencies also must reconsider their traditional business processes and organizational structures, which were born out of the industrial age. Now that we've entered the network age, we have an opportunity to take an entirely new approach, by using traditional data in unconventional ways. And, at the same time, to reinvigorate the workforce, providing a new focus on service delivery and safety.

But it is the visibility gained that holds the greatest benefit for day-to-day operations. By identifying the key business drivers, government can eliminate redundancy, reduce complexity, and drive out costs while improving efficiency. Taking an approach to information sharing that increases visibility throughout the organization allows agencies to better leverage their legacy systems first, and then make key investments for more effective allocation of funding.

Justice and public safety agencies in particular must undergo a change in attitude, moving toward the more proactive prevention and detection approach, away from a recovery and response mindset. By applying business intelligence techniques to traditional data, agencies will find they have actionable information that can help them secure their communities, and, at the same time, improve service delivery and efficiency.

About the author

Gerry Wethington, Vice President, Homeland Security and Justice & Public Safety Programs

Global Public Sector

Unisys Corporation

Gerry Wethington is vice president, Homeland Security and Justice & Public Safety Programs, Unisys Global Public Sector, responsible for leveraging the entire portfolio of services, solutions and technology products to take Unisys to a leadership position in these markets. Gerry is based in Reston, Va., and has an office in Jefferson City, Mo.

Prior to joining Unisys, Gerry served as Missouri's chief information officer (CIO) and as a member of Gov. Bob Holden's cabinet, where he led Missouri's e-government efforts to improve the delivery of government service to its citizens. He also led the development of Missouri's Adaptable Enterprise Architecture Program. Considered one of the best in the nation, this program resulted in significant savings and improved efficiency in the state's business and IT programs. Gerry is recognized nationally as a leader in the areas of government process reform, enterprise architecture, justice integration and interoperability, and project management.

Gerry served two consecutive terms as the president of NASCIO, the National Association of State Chief Information Officers. Gerry is the only state CIO to serve consecutive terms as president in the association's 35-year history. He also served as chair of NASCIO's Enterprise Architecture Committee and as a member of its Executive Committee.

Gerry was Missouri's SEARCH representative, serving as chairman and member of the Board of Directors. SEARCH is the National Consortium for Justice Information and Statistics, with representatives from all states, responsible for formulating recommendations on criminal justice policy. He served as vice chair of the membership group and chaired the Planning Committee and the Systems and Technology Program Advisory Committee.

Former Attorney General Janet Reno appointed Gerry to the Global Justice Information Sharing Advisory Commission, an advisory body to the U.S. Attorney General created to support broad-scale exchange of pertinent justice information. Gerry served as the vice chair of the commission and served on the Executive Steering Committee.

Gerry is a frequent speaker at seminars and conferences on topics related to government process improvement, enterprise architecture, technology infrastructure centralization and consolidation, homeland security, criminal justice integration and interoperability, progress and performance metrics implementation and software engineering. Some of the programs where Gerry has spoken include: CIO magazine's Strategic Initiatives Conference, the Department of Justice, Office of Justice Programs Integration Workshops, the National Governors Association (NGA) Justice Integration Workshops and Chiefs of Staff Retreat, NASCIO annual and mid-year conferences, SEARCH's Integration Symposium, FSI's State of the State's Address, technology symposiums in the states of Texas, North Carolina, Ohio, Tennessee and Connecticut, the Japanese Prefecture Government CIO Forum in Tokyo, Japan, the Missouri Police Chiefs Association Legislative Seminars and the Missouri Office of Prosecution Services Training Seminars.

Gerry holds a bachelor's degree from Westminster College, Fulton, Mo.

¹ NASCIO Compendium of Digital Government in the States 2004-2005, p 12, National Association of State Chief Information Officers, 2005.

² State News, "Trends in America: Charting the Course Ahead," August 2005.

For more information, please visit our Website at:
www.unisys.com/public_sector

Specifications are subject to change without notice.

© 2006 Unisys Corporation.

All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands or products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

