U.S. Department of Justice
Office of Community Oriented Policing Services

COPS

COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

Policing Smarter Through IT: Lessons in Enterprise Implementation

www.cops.usdoj.gov

Prepared by The Institute for Policy Research,
Northwestern University

Policing Smarter Through IT: Lessons in Enterprise Implementation

Smarter Through IT: Lessons in
ng Smarter Through IT: Lessons in Enterprise Implementation
Policing Smarter Through IT: Lessons in Enterprise Implementation
in Enterprise Implementation
Policing Smarter Through IT: Lessons in Enterprise Implementation
Policing Smarter Through IT:

(A Companion Publication to "Policing Smarter Through IT: Learning from Chicago's Citizen and Law Enforcement Analysis and Reporting (CLEAR) System")

Prepared by
Northwestern University

Wesley G. Skogan
Susan M. Hartnett
Jill DuBois
Jason Bennis

ISBN: 1-932852-38-X

This report was prepared by Northwestern University, supported by Cooperative Agreement #2002CKWXK003, awarded by the Office of Community Oriented Policing Services (COPS), U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

foreword

Policing Smarter Through IT: Lessons in Enterprise Implementation

Foreword

We are pleased to present this report on the CLEAR system. CLEAR, the Citizen Law Enforcement and Analysis and Reporting system was developed by the Chicago Police Department in partnership with the Oracle Corporation. Its focus on criminal justice data integration evolved out of the need to streamline and improve the utility of law enforcement data. The COPS Office has provided approximately $9 million for the CLEAR project in funding through MORE technology grants to the Chicago Police Department and other innovative grant programs. COPS also provided funding to Northwestern University to conduct a formal evaluation of the project, the results of which are contained within this report.

The CLEAR system is currently used regionally, but it will soon be adopted by the entire state of Illinois, seamlessly integrating a broad range of police and criminal justice functions electronically. CLEAR uses a variety of cutting-edge technologies and is credited with saving officer time, reducing overtime costs, significantly reducing the need for clerical staff, helping to solve cases through its relational database, and, increasing crime clearance rates in Chicago. It is being described as a national model for the future of police information systems and is currently being studied in Washington, D.C. and Los Angeles, California.

Just this year, the Chicago Police Department won CIO Magazine's Grand Enterprise Value Award for this forward-thinking technological undertaking. This award represents the hard work of creative police officers and benefits multiple components within the criminal justice system, including law enforcement, courts, and corrections, thus enabling them to work together towards the same goal. We hope you will find the recommendations of this report helpful to you and the members of your own agency as you keep your communities safe.

acknowledgments

Acknowledgments

Our thanks to Chicago Police Superintendents Philip Cline and Terry Hillard for their cooperation with, and encouragement of, this project. Similar support came from retired Deputy Superintendent Barbara McDonald, Deputy Superintendent Ron Huberman, and Information Services Director Charles Padgurskis. Their receptivity allowed us ongoing access to the police department and its partnering agencies in the Chicago metropolitan area. We also appreciate the cooperation of the Oracle Corporation, whose CLEAR project staffers have interacted freely with our research staff.

Also generous with their time and expertise were personnel from the Chicago Police Department's Information and Strategic Services Division, who granted us extensive time for interviews and ample access to meetings. Of tremendous benefit to the project were many officers and civilian employees throughout the department who completed several questionnaires regarding CLEAR technology and its impact on their jobs; suburban Chicago police agencies that afforded us time to interview their personnel about the CLEAR data warehouse's impact on their organizations; the Illinois State Police for allowing us to interview key people in the criminal justice integration project; and the Illinois Criminal Justice Information Authority for permitting us to interview its staff about Chicago's criminal justice integration project.

In addition, we appreciate The University of Illinois at Chicago's partnering with us in this project and for conducting formative research in the area of enhancing citizen involvement with their local police through the development of web surveys.

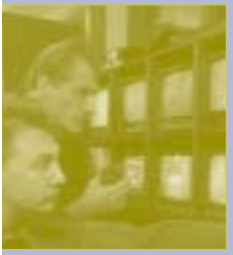


table of contents

Policing Smarter Through IT: Lessons in Enterprise Implementation

Table of Contents

one: introduction

Policing Smarter Through IT: Lessons in Enterprise Implementation

I. Introduction

THE VISION WAS TO BUILD AN ENTERPRISE INFORMATION SYSTEM - CUSTOMIZED FOR THE CPD, BUT ADAPTABLE TO OTHERS - THAT WOULD FUNDAMENTALLY CHANGE THE WAY THE ORGANIZATION DOES BUSINESS.

The information technology (IT) revolution is exploding in the criminal justice field. Police executives know that new technology can greatly expand their capacity for tactical, strategic and investigative analysis and decision making, and for managing the enterprise. Crime mapping and hot-spot analysis have become part of the toolkit of many departments. Community policing activities, such as problem-solving, have benefited from improved crime mapping and have demonstrated the value of mobile technology in moving officers from their desks to the field. Federal initiatives such as the U.S. Justice Department's Project Safe Neighborhoods depend heavily on the analysis of operational and investigative data. New data systems, such as the New York City Police Department's CompStat system, also support management accountability initiatives. Police departments are ripe for change because IT is maturing and the cost of adopting it is dropping steadily. However, observers would agree that many departments have had difficulty bringing it online in a timely and cost-effective way.

In 2001, the Chicago Police Department (CPD) undertook the development of a state-of-the-art, integrated criminal justice information system referred to as the *Citizen and Law Enforcement Analysis and Reporting (CLEAR) System*. The vision was to build an enterprise information system – customized for the CPD, but adaptable to others – that would fundamentally change the way the organization does business. The CPD developed strategic goals for the

system and the means of funding it, made hardware and vendor decisions, and designed a strategy for involving users of the system in every stage of its development and implementation. Although the CPD successfully addressed most of the development and implementation issues they faced, being an early developer of such a system certainly magnified the complexity of the task. We anticipate that other law enforcement agencies planning to incorporate advanced information technology into their daily operations will encounter these issues as well.

This report summarizes the lessons learned from an evaluation of the CPD's CLEAR system. The evaluation tracked the ways in which the CPD confronted system development and implementation issues as they emerged. At the operational level, the report discusses training, help desk and internal marketing strategies, and the incorporation of early feedback from working officers. There is also a description of organizational level issues, including scheduling roll-out of new systems, developing privacy and security policies, external data sharing arrangements and coping with diversionary pressures that threaten to get the process off track. The final section of the report discusses the importance – and difficulty – of assessing the effectiveness of new information technology in a public sector organization.

Readers of this report may benefit from CPD's experience, particularly if they are engaged in a criminal justice data technology project. The report may be useful for executives and managers in other criminal justice agencies who are eyeing the information technology revolution.

The applications comprising Chicago's CLEAR system impact three functional aspects of policing: management, criminal justice integration, and community/business partnerships. The goals for each aspect are as follows:

Police management: Promote effective resource allocation; management accountability; officer accountability; risk management and early warning; tactical and strategic planning; and fiscal accountability. The department-wide management accountability process already makes use of the new system to address crime and disorder problems, react to emerging crime trends, optimize community involvement, and manage the department's human resources. In addition, the system will soon provide predictive information for deploying officers when and where they are needed.

Criminal justice integration: Enable unified strategies to reduce crime, eliminate criminal justice bottlenecks, increase accountability among criminal justice agencies, provide a comprehensive picture of offender activity, and manage offender flow through the criminal justice system. An extensive information-sharing network already links several hundred law enforcement agencies, prosecutors, courts, and the corrections system to the CPD data warehouse. The goal is to enhance the capacity of the entire metropolitan area to "police smarter," deepen partnerships with surrounding suburbs and cities, improve the quality of criminal justice information, improve employee morale, and reduce liability costs.

Community/business partnerships: This technology is expected to advance community policing initiatives through its potential for strengthening the capacity for problem-solving, enabling community-needs assessment, and allowing for easy and convenient information sharing and intelligence gathering from the community. The CPD currently partners with residents through monthly beat community meetings and advisory committees in each of the 25 police districts. Next on the agenda is a new effort to involve residents in information-sharing and problem-solving via the Internet to supplement citizen involvement at beat community meetings.

These technology applications are expected to create safer communities, downsize administrative functions, increase management and officer accountability, and increase proactive community involvement. The various applications comprising the system are increasingly available through the intranet at the CPD, the Internet for the public, and the extranet for other government agencies. When fully realized, the system will touch every aspect of department operations and expand the borders of data sharing among other agencies at both the state and federal levels.

two: enterprise system development

Policing Smarter Through IT: Lessons in Enterprise Implementation

II. Enterprise System Development

...IDENTIFYING AND APPLYING FOR MULTIPLE STREAMS OF FUNDING IS A JOB IN ITSELF.

The CPD's experience in enterprise system development revealed that it is a process fraught with unanticipated roadblocks. Project managers may try to follow a step-by-step development process, but outside forces can upset a seemingly ironclad plan. These include funding-related issues, complex hardware decisions, vendor problems, accommodating the views of users in developing business rules, discovering internal redundancy, problems in maintaining scope boundaries, diversionary pressures, security threats, and the need to take ownership – and responsibility for – the final product. This section presents the issues and considerations encountered in building an IT system in a law enforcement environment.

Funding management

Developing an enterprise IT system involves complex financial management issues. Rarely is an agency in the enviable position of having ample funding earmarked for the project, so identifying and applying for multiple streams of funding is a job in itself. For many agencies, the problem is one of insufficient funding – "too little, too late" – but for others the situation can be "too much, too late." Grant funds may come marked "perishable" because like food, the money may have to be used by the expiration date. Worse, bureaucratic problems often mean that the money has to be spent quickly because the funding deadline is perhaps the only one that cannot slip. Too often it turns out that finding the money is just part of the battle. Grant management is a balancing act. Will the software be developed by the funding's expiration date? Will hardware be installed and infrastructure changes completed

before the money disappears? The complexity of working with grants – keeping track of expiration dates, identifying future funding opportunities, writing proposals, tracking spending – calls for a dedicated staffer to handle it.

> *Obsolescence goes with the territory, and the only way to avoid it is to do nothing at all – which is unlikely to solve any problems.*

The "FUD" factor: hardware and operating system decisions

The only certainty in the world of IT is that if you purchase something one day, it is outdated the next day. The "FUD" factor – fear, uncertainty, and doubt – permeates computer hardware and software decision-making. There is an adage about not being the first person on the boat or the last on shore, and in the world of IT, it is often hard to tell whether the boat has just arrived or is about to leave. It is hard to know whether to upgrade, adopt the newest products available, or wait for the next version of something already on the market. There are countless hardware options and even a few operating system choices, and the most well reasoned decisions can seem shortsighted when new products are announced a few months later. The prospect of obsolescence can paralyze the development process.

A project manager, for example, may hear that a much-touted new product will be introduced within six months. Armed with this knowledge, the decision may be made to delay a project until this (possibly) better generation of hardware or software hits the market. While there will always be good arguments for waiting, there is also much to be said for taking the plunge and getting a project underway.

Our experience is that there is no easy solution to this quandary. We have seen decisions to stay with an older version of an operating system result in new applications functioning improperly. We have also seen the decision to go with a newer product that provides desirable features reveal hardware deficiencies that cancel out some of the expected gain. The lesson is that any dynamic system, by definition, is constantly changing. Obsolescence goes with the territory, and the only way to avoid it is to do nothing at all - which is unlikely to solve any problems.

MISSED DEADLINES AND BROKEN PROMISES BY VENDORS CAN TRIP UP ANY PROJECT.

Vendor problems – the need for Plan B

In many ways, a project is only as strong as its vendors. Missed deadlines and broken promises by vendors can trip up any project. Because the components list for an enterprise system is so lengthy – hardware, software, network providers, consultants, and the like – it may be necessary to deal with hundreds of vendors and myriad details. From a time and knowledge standpoint, it is often convenient to identify one vendor offering customized procurement services for if something goes awry with a subvendor, the primary vendor will be able to quickly turn to the next source and keep the project moving.

But what if something goes wrong with the procurement vendor? For a big-city agency, the bankruptcy of a procurement vendor can be devastating. Municipal governments typically labor under labyrinthine purchasing procedures and approval processes, and the failure of a procurement vendor to continue in its role can bring development to a halt.

The CPD, for example, had difficulties with a procurement vendor that failed to pay its subcontractors, and the flow of hardware, software, and consultant services needed to keep the project moving dried up. Acquiring the equipment or software for which funds were earmarked and available became an exercise in creative thinking; critical items to keep development on pace needed to be sought from alternate sources, some of who were still demanding payment. Devising "Plan B" should be an integral part of "Plan A."

In-house development vs. outsourcing

The temptation for large law enforcement agencies to develop information systems in-house can be very strong, especially for those with IT departments. Adding to the temptation is the belief that nobody understands the business of a police department but the police. And, if added to the equation, earlier experiences with systems developers have resulted in an application that was less than ideal (and that is a very frequent experience), the decision to rely on consultants and outside developers can be a hard one to reach. But just as law enforcement officers do not encourage citizens to take the law into their own hands; neither should they expect to be able to develop internally an integrated information system aimed at changing the way they do business.

The CPD almost succumbed to the temptation. In fact, a team of officers was, for a time, busy developing the most technologically complicated and vital application on the drawing board. Then, a new project leader – fresh from the outside – led the department to partner with a management systems software developer, thereby merging systems knowledge with knowledge of the CPD's system. However, when possible, CPD employees, both sworn and civilian, co- develop applications, and at all times CPD insiders provide their expertise in developing the business logic coded into the software.

Knowledge transfer

> ...THE DEVELOPMENT OF A STRONG IT UNIT SHOULD BE CONSIDERED AN INVESTMENT IN THE INFRASTRUCTURE OF THE DEPARTMENT.

Once a working relationship is established with consultants and developers, a hurdle that appears on the horizon is how to end the relationship in a timely and tidy manner. A required part of a project development plan should be the target date by which internal IT personnel become fully familiarized with the application so that responsibility for upgrades and maintenance can be "offloaded" from the development specialists - especially in law enforcement agencies, which operate around the clock. Application development and maintenance responsibilities do not end when the switch is turned on. Inherent in enterprise systems are the continuing efforts to deal with or adapt to new requirements. Among the things that can be handled by in-house IT staff are documentation, training, hardware upgrades, system-bug resolution, and maintenance.

In the public sector, diminishing reliance on vendors may be a matter of necessity. Grant-based funding may specify that monies are to go for development, and not routine operations. Even if this is not specified, it is not likely that grant funding will be available for long-term maintenance and upgrades. Therefore, a plan to foster the development of an in-house skill pool should be in place at the beginning of the project. It is unlikely that an organization supporting a complex enterprise system will be able to become completely self-reliant in this era of ever-evolving technologies, but the development of a strong IT unit should be considered an investment in the infrastructure of the department.

Eyeing the big picture

Few people would sit down to work on a complicated jigsaw puzzle without first having a mental picture of the finished product – this is why publishers put the picture on the cover of the box. Likewise, no one should expect to create an enterprise system without knowing what parts will comprise it and how they should fit together. This does not imply that project managers must fully understand the technical aspects of the system, but it is imperative for them to understand the functional components that make up the system. This simple advice may seem self-evident, but knowledge gaps can exist.

We observed, over a two-year period, the apparent segregation of a key part of the CPD's enterprise system. Month after month, development of this application progressed without review at project management meetings. Little groundwork was laid for the eventual inclusion of this application into the system framework, and one of its key developers seemed not to realize that the application would ultimately interact with other software modules. It is easy now to trace the roots of this problem because development of the segregated system began long before the larger IT initiative was undertaken. Only as deadlines approached did it become clear that someone needed to take a step back to view the big picture. The application was finally absorbed into the mainstream project, but at a very late date.

Infrastructure capacity

As applications are added to an enterprise system, increasing demands are made on the organization's servers. When new demands are piled on the hardware over time, capacity limits may be reached unexpectedly, taking IT managers by surprise. Users feel the impact as they experience maddening delays in system responsiveness. This is

a situation that no IT manager wants to be faced with, because it can take considerable time to identify, purchase, and launch new servers to resolve the problem. A proactive awareness of server needs is to be advised.

Another important infrastructure issue is whether to build or lease a telecommunications network. While building one's own network may seem like a good idea in terms of customizing the system to an agency's specific needs, one can also expect an outdated system by the time it is installed and ready for use. Keeping pace with technology developments in the telecommunications field is particularly expensive and time-consuming. By leasing a system from a reliable vendor, an agency can expect continual updates to their product, providing them the most up-to-date system possible.

Managing "scope creep"

“Scope creep” is a term for the practice of adding features or capabilities – new functionalities or modifications of those already underway - during an application's development stage. In the CPD, most scope creep seemed to come about as brainstorming sessions and system tests by experienced officers identified new potential in the technology being developed.

Many officers come to these sessions unconvinced that computers can actually help them do their job better, and they are not shy about identifying shortcomings in the application that is on the table. Some scope creep is thus desirable, but the key is keeping it under control, for it predictably can result in implementation delays and additional cost.

Controlling scope creep is also a balancing act. While there is no question about the wisdom of staying on schedule and within budget, constantly denying requests for added features runs the risk of, at the very least, alienating once-interested stakeholders, and in the worst-case scenario, implementing an application that falls short of what the organization needs. Determining a reasonable scope for an application and sticking as close to it as possible is perhaps the only way to deal with scope creep. And as was done in the CPD, setting aside, but not losing sight of, upgrades and new features for later versions can help keep scope creep under control.

IT IS NOT HARD TO IMAGINE THE DETRIMENTAL EFFECT THAT LACK OF COORDINATION AND INFORMATION SHARING CAN HAVE ON A SYSTEM – INTEGRATION HEADACHES, FUNCTIONALITY OVERLAPS, AND UNNECESSARY EXPENSE, FOR EXAMPLE.

Information silos

"Information silos" is a term we heard quite a few times during the course of the CLEAR system evaluation. An apt metaphor, developing various modules of an enterprise system in isolated groups hampers timely coordination and communication among units. It is not hard to imagine the detrimental effect that lack of coordination and information sharing can have on a system - integration headaches, functionality overlaps, and unnecessary expense, for example.

We saw a classic example of the silos problem in the CPD. Months into developing a very ambitious and comprehensive personnel-functions application, it was discovered that a client-server application that had been developed in-house was already in use, collecting information and providing reports that were closely related to

those forthcoming from the still-under-development personnel system. And, upgrades and new functionalities were continuing to be developed for this independent system. While the software developed in-house was customized for a single division within the department, the developers of the client-server application and the personnel system did not get together to discuss the similarities and differences among the applications until well into the enterprise system development phase. Eventually, plans were made to web-enable the in-house system so it would have the "look and feel" of the other applications under development.

ANOTHER POTENTIAL OVERSIGHT THAT CAN OCCUR... LEAVING IMPORTANT CONSTITUENCIES OUT OF THE PLANNING AND DEVELOPMENT PROCESS.

Another potential oversight that can occur when development takes place in silos involves leaving important constituencies out of the planning and development process. A case in point is evident in the CPD: the comprehensive personnel management application under construction not only promises to transform the department's management processes, but it may also help drive the department's accountability efforts – yet staff members in the management accountability unit of the department know virtually nothing about the enterprise system or the applications that comprise it.

Security

The importance of security need not be explained to a law enforcement audience. Agencies must protect themselves from at least three different types of breaches: internal, when department personnel gain access to information for which they are not authorized; external, brought on by viruses and recreational hackers; and terrorist, the potentially

devastating intrusion or destruction on the minds of many in this post-September 11th environment. Role-based security checks can prevent users from acquiring information that is not appropriate; for example, only officers who have supervisory capacity are able to view and approve and various reports based on their functions within the department.

Commercial firewalls can counter hacker attacks and viruses, although they need constant attention and upgrading. The pervasive terrorist threat, on the other hand, requires preemptive action of a different sort. A secure, offsite backup facility must be identified and this, too, can be challenging. Finding a site that can back up a large, complex system and that is potentially a lesser terrorism target than the original facility can be difficult in the current climate.

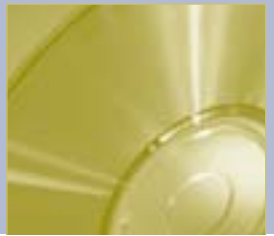
Setting realistic deadlines

It is important to have completion goals for any development project, but competing forces may intervene to destroy any hope of meeting conservative deadlines. This is especially true in law enforcement agencies, as external life-and-death factors can redirect both manpower and organizational priorities. During the time we have been watching development of the CPD's enterprise system, local, national, and internal events have had significant impacts on personnel, development priorities, hardware availability, and deadlines.

Thus, deadline adjustments are to be expected, and they should be made judiciously and realistically. When unrealistic deadlines are imposed, tremendous pressure is put on the development team, creating an atmosphere in which shortcuts are taken and mistakes made. We occasionally saw deadlines imposed that everyone knew were impossible to meet, perhaps out of frustration or a management tactic. Deadlines that cannot be met have an effect on quality and reliability, and should be avoided.

three: enterprise system implementation

Policing Smarter Through IT: Lessons in Enterprise Implementation



III. Enterprise System Implementation

Operational level

The CPD's experience revealed five facets of implementation at the operational level that had a significant impact on successful application deployment: conducting a physical capacity assessment, generating internal marketing, capturing officer feedback, providing officer training, and establishing a user support process.

Physical capacity assessment

The untimely realization that the physical facilities available in the field cannot accommodate a new IT application can be a critical roadblock to a successful application launch. Once an application's development plan is in place, it is important to conduct an assessment of the physical capacity of stationhouse facilities' hardware, software, lighting, wiring and other infrastructure elements, to make sure that all of the pieces are in place for a successful application roll-out.

In the CPD, for example, this was carried out by officers who went to each of the department's stationhouses to examine their capacity to accommodate the enterprise system. They assessed existing hardware and the physical capacity of the stations to accommodate the users who would need to access the system. The assessment consisted of room-by-room examinations (front desk area, sergeants' offices, interview rooms, tactical office, lockup, radio room, etc.) of available space, existing computer hardware and operating system configurations, the availability of internet connectivity ports, and even the station's power supply and wiring. Rarely are stationhouses

prepared for a major new application. While the following recommendations are generally applicable, they are by no means a guarantee of implementation success, and members of the development team with a good understanding of system and user needs must be involved in capacity assessment in a hands-on fashion.

Assessment team: It is vital that the team or individual selected to conduct assessments have, in addition to ample policing experience, a wide array of skills, including knowledge of hardware and current technology trends, an understanding of the application's hardware requirements and impact on space utilization, and a basic knowledge of electrical wiring. It is important for the assessment team to be aware of the organization's plans, such as when stationhouses are scheduled to be renovated or replaced, as well as the effect that these plans will have on an application's launch. The assessment team must be able to discern between a facility's true equipment needs and officers' well-meaning attempts to fill their wish lists.

Safety: When performing facilities assessments, officer safety must be kept at the forefront. Astute assessment teams will recognize potential safety and operational advantages of certain types of hardware. For example, flat-panel computer screens may be preferable to traditional monitors because they take up less space and provide a less-obstructed view of offenders during arrest processing. Power outlet location also requires careful consideration to reduce safety concerns – especially in arrest processing rooms. Outlets located too far from workstations or too close to prisoners could place lengthy power cords within prisoners' reach, leading to processing disruptions, injury to prisoners or officers, or equipment damage. Also of concern in the arrest processing room is furniture installation: computers must be bolted to desks that are secured to the floor. Care must be taken when considering furniture options, as not all tables and computers can be easily anchored together.

Application design requirements: Another key element of a facilities assessment is a thorough understanding of extenuating circumstances that impact application utilization. For example, in the CPD, juvenile arrests must be

processed in a separate room using a computer dedicated to juvenile-offender processing. In contrast, arrest processing of adults can take place in numerous processing rooms with shared computer stations. Hence assessments must determine the number of computers needed for stand-alone tasks, as well as a count of those to be used for shared officer tasks. Providing sufficient and strategically placed computing resources can reduce user dissatisfaction with new applications.

A facet of the CPD's automated case reporting system further highlights the need to consider every possible impact that an application may have. In the near future, officers will be able to wirelessly complete and submit reports using data terminals mounted in their cars. This advance makes the availability of spare charged portable data terminal (PDT) batteries very important. Aware of this, the assessment team needed to determine the minimum number of PDT batteries and chargers to accommodate each district's personnel roster, as well as the optimal type of battery to be used in Chicago's frigid winter climate. Climate also affected the choice of computers, for flat-screen LCDs have a habit of cracking when the temperature in the car drops too low.

Anticipate issues: A good physical capacity assessment should anticipate potential problems when a complex computerized system is deployed. These can be basic environmental issues as well as technology-related obstacles. One such unexpected environmental problem – dim ambient lighting combined with dingy walls – limited the initial effectiveness of the CPD's new mugshot system at several sites. In the technology category, outdated PC operating systems, which are easy to overlook because they are, by nature, operating in the background, caused aspects of newly developed applications to malfunction.

In addition, ensuring that virus protection software is up-to-date on each workstation is critical. System functionality can be brought to a halt by an undetected virus.

Internal marketing

> RANK-AND-FILE RESISTANCE TO NEW APPLICATIONS CAN BE DIMINISHED BY A WELL-CONCEIVED MARKETING CAMPAIGN.

Another important facet of implementation at the operational level is the use of internal marketing to generate early excitement about an IT application. Rank-and-file resistance to new applications can be diminished by a well-conceived marketing campaign. In the past, newly introduced automated systems sometimes met significant resistance in the CPD, especially among veteran officers with limited computer experience. The department's current approach is to raise awareness of applications under development well in advance of implementation. Early internal publicity can highlight the project's benefits for the average officer.

Marketing efforts should try to derail predictable complaints such as, "It'll take me longer to fill out a report online" and focus on the advantages offered to users by the new system, such as the increased availability of accurate data and increased report legibility, the ease of making corrections, the convenience of drop-down menus, the ability to move information from form to form, and the like. Care must be taken, however, not to "oversell" the new application and foster unrealistic expectations. Marketing campaigns can consist of memos and promotional literature or videos, coupled with articles and information posted on law enforcement web sites to help generate interest and a sense of pride in being a leading-edge department. Kickoff meetings provide an opportunity to create excitement among those closest to the application, with the possibility of trickle-down effects to other parts of the department. If nothing more, these measures may stimulate officer dialogue about a new application, making them feel a part of what is happening and better prepared for changes in their day-to-day tasks.

Testing and feedback

> *... IT IS IMPORTANT TO CREATE AN AVENUE FOR OFFICERS TO PROVIDE ONGOING FEEDBACK.*

Garnering feedback from future users is an ongoing process in the CPD. It routinely begins in the conceptual design stage, continues during developmental brainstorming sessions with potential users, and takes on increasing significance during often extended implementation periods. As late as the pre-launch phase, groups of officers can provide feedback on test versions of an application, and pilot test it in the field. Officers have an incentive to provide critical feedback, knowing that they will soon be routinely using the application. Most officers appear eager to provide open and honest feedback about an application's strengths and weaknesses.

Our observations in the CPD yielded a few key factors related to testing and feedback. First, care must be taken to select skilled, conscientious, and open-minded officers and allow them adequate time to thoroughly investigate and evaluate all of an application's functions. The more time spent evaluating, the more likely it is that flaws will be found and corrected before implementation. While it may seem unnecessary to point out that follow-through is important when eliciting feedback, we observed that for one of the CPD's applications, officers were encouraged to fill out feedback forms that were never collected.

It is recommended that a team of testing officers be assembled over a predetermined period of time (days, weeks or months, depending on the complexity of the application) and be given the opportunity to focus solely on testing the application. If this is not feasible, general feedback from users in the field can be fruitful, but it is apt to be less

systematic. Testers who are asked to test an application during their downtime – rather than in a formal testing setting – are not apt to provide in-depth feedback. It may be necessary to hold roll call reaction sessions or other types of gatherings to elicit meaningful recommendations. Finally, after full implementation, it is likely that minor bugs and glitches will surface. Therefore, it is important to create an avenue for officers to provide ongoing feedback. An effective option is to provide an e-mail link for reporting errors so that officer feedback can be sent directly to those in charge of maintaining the application.

Training

Successful implementation is dependent on adequate user training. The CPD has several training options, all with varying degrees of cost, time, and effectiveness.

Roll call training: A basic form of user preparation is roll call training, which relies on streaming videos displayed in the roll call room, departmental memos, handouts, or presentations by trainers. Because roll call can bring officers and civilian personnel together in the presence of a supervisor, it is a cost-effective method for delivering instruction on less-complex applications, and it is especially effective for introducing upgrades to existing systems. We found this training delivery method to be most effective when a trainer was on hand during the presentation to answer questions about the new application and as necessary, remained available for a period of time afterward to provide hands-on assistance.

Classroom sessions: Training users on more complicated applications usually requires hands-on instruction at an appropriately equipped site, with skilled trainers delivering a customized curriculum. For example, the automation of the entire arrest process in the CPD requires one full day of training for every police officer, and an additional day of

training for all supervisors and managers. Training on this scale is a costly venture and, in a big city agency, a logistical feat; nonetheless, this configuration can be essential for complicated systems that are vital to the organization's operation. It is also important to have several trainers available in the classroom to provide individualized over-the-shoulder attention to participants, as needed, to allow the primary instructor to keep the lesson moving along.

On-the-job training: On-the-job training can be used to familiarize officers with new applications in their work environment at the time of implementation. It requires a carefully assembled team, often consisting of one or two trainers and a technical expert to handle troubleshooting. This method generally captures officers' attention because of the individualized attention and immediacy of the setting. In the CPD, for example, it was possible for training teams to personally instruct lockup keepers in the use of a new digital mugshot system as they continued to process arrestees. Care should be taken to ensure that all "day-off" groups are accommodated. District personnel on each of the three shifts should be identified to provide later instruction to those who were not present for instruction delivered by the trainers.

Train the trainers: In this instructional option, designated officers are trained in a classroom setting and, once familiar with the application, are sent back to their respective units to train fellow users. The CPD, for example, trained designated representatives from suburban Chicago police agencies on use of the data warehouse in a half-day classroom session at police headquarters. Approximately 20 participants attended each session. Those participants, usually two per agency, in turn trained others in their respective police departments. While this is a cost-effective method, it is difficult to maintain quality control of the curriculum and its delivery.

Supplemental training material (user manuals or bulleted tip lists) effectively augment training of all kinds. Lists of problems and solutions or answers to frequently asked questions are useful because they can be posted in officer workspaces to provide a quick reference. Training manuals that detail instructional sessions or more general user manuals can function as comprehensive reference tools. In the CPD, officers with limited computer experience seem to prefer having printed user manuals to remind them how to use aspects of the application as opposed to more seasoned users who are comfortable with online help options. More proficient computer users are comfortable with tip lists and online supplemental materials.

> ...KNOWING WHO HAS BEEN TRAINED IS KEY.

An important training component is tracking; knowing who has been trained is key. Without an accounting system in place it is nearly impossible to know whether all users have undergone training and difficult to determine how long to continue offering training sessions and whom to target. Accurate recordkeeping can prevent situations in which users claim that they do not know how to use an application because they were not made aware of training sessions.

Finally, it is advisable to think through a new application's dependencies on other applications and whether users are adept at using them. If the other systems are complicated by or changed in conjunction with a new application's launch, it may be necessary to include instruction on how to use them as a part of training for the new application.

Multi-tiered help system

Successful implementation of any IT application calls for a multi-tiered help system, allowing users to quickly access accurate information.

Self -help resources: One line of support is help functionality built directly into an application so that with a few clicks of the mouse, officers can find answers to their questions. Another self-help option is the use of reference tools – training booklets, user manuals (printed or online), and a printed troubleshooting list. Self-help resources are especially advantageous for personnel who may be covering for a co-worker with different day-to-day duties.

> A RELIABLE SYSTEM FOR CALL-BACKS MUST BE ESTABLISHED...

Go-to person: In some cases, self-help resources will not be adequate, and it is advisable to appoint several liaisons or "go-to" persons at each facility who can clear up confusion and provide user support. The advantage of having such a designee is that officers often feel more secure about using new applications when a knowledgeable co-worker is available to answer questions and help them troubleshoot problems. However, identifying a willing "go-to" person available on each shift may be difficult, as this is usually an added responsibility for an already-hardworking person. At times, this person will be unavailable to respond to user issues in a timely manner. Another pitfall of relying on a go-to person as a primary resource is that personnel transfers, medical leave, or retirement can leave a unit unsupported.

Help desk: A thoroughly trained and well-managed help desk is a valuable asset to users. The help desk is a key contact point, for callers expect resolution of their problems when they make the call. Without a reliable help desk, users can overlook vital features and lose the benefits of new applications. A help desk can be a vital support system in organizations such as law enforcement agencies, which operate around the clock.

Help desks have great potential for enriching the user experience. However, if the help desk is not well managed or adequately trained, breakdowns in procedure and performance are likely. As in any customer-client service situation, callers expect a prompt, knowledgeable response. A coordination challenge unique to law enforcement agencies is related directly to the nature of officers' jobs. Because officers spend much of their time in the field, it can be difficult for help desk personnel to reach those who require return telephone calls to resolve issues. A reliable system for call-backs must be established or the help desk system will not be an effective resource.

THE IMPORTANCE OF CONDUCTING A THOROUGH AND DETAILED PROCESS-MAPPING OF THE ORGANIZATION CANNOT BE UNDERSTATED.

Over-reliance on developers or vendors is another pitfall in operating a help desk. When a new application is launched, it is likely that help-desk staffers will not have sufficient experience to troubleshoot all problems. As a result, it is likely that the help desk will rely heavily on developers and vendors for higher-level problem resolution. It is vital that comprehensive training be offered to help-desk personnel so that the need for external support is diminished. That said, as the number of applications introduced in an organization increases, help desk representatives may find it difficult to maintain a high level of familiarity with each computer program. To keep the help desk functioning at a high level, it is advisable to create a searchable knowledge database – a compendium of solutions that have been reached for previous queries.

Good internal communication is also important for help desk effectiveness. Help desk personnel should be among the first to know when system maintenance is scheduled and when systems go down. Help desk administrators should be aware of application deployment schedules so that they can provide adequate personnel to meet

anticipated increases in calls. Tallies should also be kept on recurrent questions, because later analysis may reveal needed changes to programs or new areas of emphasis in training.

Organizational level

Based on our observations in the CPD, four organizational-level issues deserve mention as considerations when developing an enterprise system in a law enforcement environment: scheduling, privacy and security mechanisms, external data sharing arrangements, and diversionary pressures.

We have seen countless unexpected events undercut carefully crafted schedules and impact timely IT implementation. We learned that internal unit coordination is essential, that buy-in is much greater with the inclusion of stakeholders in the planning process, and that unanticipated personnel changes can dramatically alter implementation schedules. Adequate privacy and security mechanisms need to be in place, external data sharing arrangements require in-depth consideration, and lastly, diversionary pressures always emerge when they are least expected. The following section discusses these organizational-level implementation issues.

Setting schedules

When developing a large IT project in a complex environment, developers usually start working on many application modules that will eventually be merged into a complementary system. Because these applications are often dependent on one another, roadblocks in one can create a chain reaction that stalls advances on many other applications. These hold-ups can appear to be terribly large and troublesome and are often linked to some overlooked step during the development phase. Creating or fixing some of these steps can be costly, complicated, and time consuming. Anticipating the unexpected is difficult. Predicting launch dates for applications with

interdependencies is difficult. The importance of conducting a thorough and detailed process-mapping of the organization cannot be understated. Each unit, person, and function should be accounted for during the process-mapping task. By looking at department needs, gaps, and overlaps, problems can be identified and addressed before the implementation stage.

Setting schedules for implementation must also take into account personnel changes that may take place within the organization. Large police departments make personnel changes often and with little notice. Officers working on IT projects hope to be promoted, and this usually leads to new assignments. Others will retire, often with little advance notice. This environment can hamper the successful implementation of an IT project. A single person should not be expected to carry out the critical tasks of project implementation. Relying on people who may be put back on the street or promoted can spell disaster for such endeavors. While input from officers is important and necessary, it is a good idea to have project managers that do not disappear in the night. Finding people in the organization who can sustain their positions throughout the length of the implementation phase is critical to adhering to project schedules.

Developing security and privacy policies

Criminal justice agencies developing an IT system are responsible for anticipating privacy and security issues at many levels. While data sharing holds tremendous promise in terms of problem-solving, predictive analysis and cost-effectiveness, inherent in it is the ongoing threat of revealing data inappropriately or violating citizens' rights. Prior to implementation, policies will need to be developed to balance officers' need for information with the risk of data misuse. At every level, policies must be in place that determine who should have what information under what circumstances.

Increased information, used properly, can translate into increased case clearances and, even better, increased crime prevention. (This assumes that the police department is properly deploying officers and communicating with residents at a rather sophisticated level.) However, when communicating with residents, there are important factors that go into deciding what information is useful to them and what information may be violating others' rights to privacy. Security and privacy policies need to be created for internal use, as do policies that determine what data can be safely shared outside the department. Each unit and rank should have access to information at levels pre-determined by their supervisors.

INCREASED INFORMATION, USED PROPERLY, CAN TRANSLATE INTO INCREASED CASE CLEARANCES AND, EVEN BETTER, INCREASED CRIME PREVENTION.

Additionally, accountability systems must be created to ensure security of the data. A system that monitors and regularly checks data usage is critical to maintaining the integrity of the information in the system. Policies must be set concerning the level of access available to personnel at various ranks, and under what circumstances management and personnel data can be accessed. It is very important to identify the circumstances under which existing crime and arrest records can be *modified*, a vital point for maintaining organizational integrity.

Policies need to be developed for handling cases of data misuse, when it occurs. This means that each system user should have a unique identification number that controls his or her access to information. This way each data query can be linked back to the person conducting the search. Only when individual officers know that they will be held accountable for their behavior can an organization have confidence that the majority will properly utilize the information. The system should be able to detect any unusual activity.

We observed one example of this which involved an officer who was questioned about why he was making so many queries to the system. While this activity was not inherently wrong, it was unusual. In this case, the officer was conducting queries for many other officers because they did not know how or want to use the system. While this did not point to data misuse, it did uncover the need for more work in addressing officers' resistance to using the technology or the need for retraining.

WITH THE NEED FOR INCREASED SECURITY FROM OUTSIDE THREATS HAS COME THE PARALLEL NEED FOR SHARING INFORMATION WITH OTHER AGENCIES.

Finally, criminal justice agencies are frequently called upon to expunge themselves of data. Making data "disappear" is not the instinct of database developers, but it may be a legal requirement that protects the rights of juveniles, people who are found innocent, or citizens who have been the target of police investigations. Data that is held in one place is easier to expunge than data that spreads ("propagates") itself around to many discrete corners of the organization. This should be taken into account in database planning. The question of whether backup and archived data must be somehow expunged is a thorny one, but one that also must be considered.

External data sharing

Most police departments have tightened their security practices in response to the threat of terrorism. With the need for increased security from outside threats has come the parallel need for sharing information with other agencies. The more information available to an agency, the better equipped it is to deal with emergency situations. In addition, the usual routines of police work are more effective when a wide network of information is available because like terrorists, everyday criminals pay no attention to municipal boundaries.

By implementing the CLEAR system, the CPD has taken the lead in a large-scale criminal justice, web-based information-sharing project that involves several hundred law enforcement agencies, prosecutors, and federal agencies. They have access to a growing body of crime, arrest, and investigative data that is being centralized in the CPD's computers. Several key issues that emerged as this criminal justice integration project were noted in the evaluation.

It turns out that building a solid enterprise system to support a cooperative network of information sharing is not enough to make it happen. The system must be marketed to potential users in a manner that demonstrates both the benefits to other agencies and the ease of using the system. This requires knowing users' needs, aggressively pursuing potential users, and providing start-up and ongoing help to keep things moving.

For example, a retired police lieutenant holding a civilian position within the CPD serves as a full-time "salesperson" for the system. He approaches surrounding communities to explain and demonstrate the system, and follows up on all inquires by other agencies. A fair amount of technical hand-holding is provided for those who need it. Participating agencies can send officers to the CPD for specialized training at no cost. While this is a task-intensive outreach effort, having data collected by and accessible to surrounding communities has had a profound impact on clearance rates and has led to the development of new partnerships between those agencies and the CPD.

For other jurisdictions, getting information from the CPD has become just a "click on the keyboard," as opposed to the past effort and expense involved in sending someone downtown to wait in line for 'this' or 'that' file folder. Neighboring agencies are solving serious crimes in a much shorter time period using information from the CPD's data warehouse. Feedback to-date supports the value of the external data sharing endeavor, despite its implementation challenges.

To make an integrated data sharing project work, the enterprise system behind it must be easy to access by other agencies, yet also be secure from inappropriate use. Experience has documented the critical importance of knowing who is accessing what data, where, and when. Every user has a unique identification number that must be used for each and every data query. System training stresses the importance of reporting any potential misuse of the data warehouse information. In one instance, a cooperating department found a CPD data warehouse printout in the home of an offender. User accountability procedures built into the system enabled the CPD to identify the suburban officer who had printed out the report, and the entire matter is being carefully investigated. While such incidents are optimally infrequent, the importance of having a system in place to detect such behavior cannot be understated. Any department that holds important and personal information must be able to ensure that it will be used appropriately, and that those who misuse the information will face serious consequences.

EXPERIENCE HAS DOCUMENTED THE CRITICAL IMPORTANCE OF KNOWING WHO IS ACCESSING WHAT DATA, WHERE, AND WHEN.

Adapting to diversionary pressures

One of the big challenges police departments face when initiating any new IT development project is being able to keep officers and resources slated for the project in place for the duration. This is difficult because policing is so inherently reactive to events outside its control, and also because the public has little interest in the improvement of back office operations if it appears to come at the expense of responding to emergencies. As a result, over time, the CPD has taken on strategic initiatives that are in some ways at cross-purposes with IT development. Like any

metropolitan department faced with the formidable task of addressing high crime rates, the CPD has had to redeploy to on-the-street assignments officers who are key players in the development of IT projects.

Training is a labor-intensive part of a major IT initiative, but in a busy department relatively few officers can stand down from duty at a particular time. When officers' and supervisors' work assignments are in flux, carefully crafted planning and training schedules can come undone overnight. This also applies to deadline-bound application developers who are called on to regroup and address more immediate and pressing problems facing the department. These situations will present problems in smaller departments as well, since they have fewer people to redeploy. Any police department planning an IT system needs to consider the reactive nature of the department's workload and schedule flexibility into the project implementation phase to accommodate both internal and external diversionary pressures.

ANY POLICE DEPARTMENT PLANNING AN IT SYSTEM NEEDS TO CONSIDER THE REACTIVE NATURE OF THE DEPARTMENT'S WORKLOAD AND SCHEDULE FLEXIBILITY...

four: assessment

Policing Smarter Through IT: Lessons in Enterprise Implementation

IV. Assessment

> NEW PROJECTS AND NEW EXPECTATIONS MUST BE BACKED UP BY SUPERVISORS...

Organizational assessment

Serious self-assessment is not easy in any organization, yet it is a critical step to knowing whether an initiative is making a difference in operations or helping an organization meet its goals. A new IT project may look impressive, but knowing whether a department functions any better as a result requires deeper analysis. There may have been a consensus that the old system was not working and great effort put into devising a new one, but the final step of gauging the effectiveness of the solution needs to be taken as well. Oftentimes the emphasis seems to be on doing the work, but not on measuring whether the work has made a difference in department goals and objectives. IT projects often begin with lofty goals, promising efficiency, speed, increasing accountability, and the reduction of crime. Only a detailed self-appraisal will uncover whether these goals have been achieved.

Officer assessment

Equally important in the implementation of an IT project is the creation of an accountability structure that matches officer performance measures with new job expectations related to the technology. This is true for any new project. Officers have seen many projects come and go, and are often hesitant to do their work differently simply because new technology has appeared in their stationhouses and patrol cars. Even with training, officers who are not accustomed to using technology may quickly revert back to old ways of doing things or become dependent on a co-worker viewed as the stationhouse "computer whiz" to conduct their queries.

New projects and new expectations must be backed up by supervisors who have an expectation that officers will be working in non-traditional ways. These new expectations should take the form of new performance measures that supervisors take seriously and utilize when making recommendations for officer salary increases and promotion. The impetus should come from the chief's office in the form of orders or directives underscoring the importance of the new project. Officers should know that the department is serious about the project and that it will be measuring appropriate skills and behaviors to ensure project success.

five: conclusion

Policing Smarter Through IT: Lessons in Enterprise Implementation

V. Conclusion

The adoption of information technology at the enterprise level is a strategic decision and it does not take place in a vacuum. The CPD's IT plan reflected its problem-solving orientation, which stresses "intelligence-driven" policing, and an internal accountability process that "manages for results." Crime analysis is a line function, and not a staff function, for rapid deployment and relentless real-time assessment requires nimble technology and up-to-date data in the hands of those who are actually doing the work.

...RAPID DEPLOYMENT AND RELENTLESS REAL-TIME ASSESSMENT REQUIRES NIMBLE TECHNOLOGY AND UP-TO-DATE DATA IN THE HANDS OF THOSE WHO ARE ACTUALLY DOING THE WORK.

The CPD's commitment to metropolitan (and now statewide) data integration reflects the new reality of American cities: close-in suburbs are facing serious crime problems, drug markets are metropolitan-wide, and the spread of gangs is closely associated with both. The CPD's plan to involve community members, and the extensive network of community activists that has built up over the past decade, reflects its commitment to two-way information sharing as part of its community policing program. New information technology thus supports the transformation of the organization and helps it adapt to changes in its environment. Both are good reasons to consider the role that technology can play in helping police meet the challenges of the 21st century.

resources

Policing Smarter Through IT: Lessons in Enterprise Implementation

Resources

All community policing and information technology publications produced by Northwestern University can be viewed at the following web site: **www.northwestern.edu/IPR/publication/policing.edu**

Harris, Kelly J. and Romesburg, William H., Law Enforcement Tech Guide: How to plan, purchase and manage technology (successfully!). A Guide for Executives, Managers and Technologists. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services, 2002. **www.cops.usdoj.gov**.

SEARCH, The National Consortium for Justice Information and Statistics. **www.search.org**

Information Technology Initiatives (*The Information Sharing Resource for the Justice and Public Safety Communities*), U.S. Department of Justice, Office of Justice Programs. **www.it.ojp.gov**

Justice Standards Clearing House. U.S. Department of Justice, Office of Justice Programs. **www.it.ojp.gov/jsc**

The Global Justice XML Data Model (GJXDM). U.S. Department of Justice, Office of Justice Programs. **http://it.ojp.gov/topic.jsp?topic_id=43**

The National Criminal Intelligence Sharing Plan. U.S. Department of Justice, Office of Justice Programs. **http://it.ojp.gov/topic.jsp?topic_id=93**

U.S. Department of Justice, Office of Community Oriented Policing Services. **www.cops.usdoj.gov**

Policing Smarter Through IT: Lessons in Enterprise Implementation

For More Information

U.S. Department of Justice
Office of Community Oriented Policing Services
1100 Vermont Avenue, N.W.
Washington, D.C. 20530

To obtain details on COPS programs, call the COPS Office Response Center at 800.421.6770

Visit COPS Online at www.cops.usdoj.gov

Created: August 11, 2004 **e07042404**
ISBN: 1-932582-83-X