



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

(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

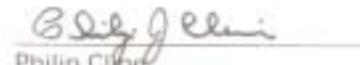
We are pleased to present this report on the CLEAR system. CLEAR, the Citizen and Law Enforcement Analysis and Reporting system was developed by the Chicago Police Department in partnership with the Oracle Corporation. Its focus on criminal justice data integration evolved out of the need to streamline 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.



Carl R. Peed
Director
Office of Community Oriented
Policing Services (COPS)



Philip Cline
Superintendent
City of Chicago Police
Department



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 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. We wish to acknowledge Dr. Debra Cohen, our COPS project manager, whose dedication, substantive feedback, and editorial support contributed to the publication of this report.

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

Foreword	i
Acknowledgements	iii
I. Introduction	1
II. Enterprise System Development.....	7
Funding management...The "FUD" factor: hardware and operating system decisions	
...Vendor problems – the need for Plan B	
In-house development vs. outsourcing...Knowledge transfer...Eyeing the big picture	
Infrastructure capacity...Managing "scope creep"...Information silos...Security	
Setting realistic deadlines	
III. Enterprise System Implementation.....	19
Operational Level	
Physical capacity assessment...Assessment team...Safety	
Application design requirements...Anticipate issues...Internal marketing	
Testing and feedback...Training...Multi-tiered help system	
Organizational level	
Setting schedules...Developing security and privacy policies	
External data sharing...Adapting to diversionary pressures	
IV. Assessment	37
Organizational assessment...Officer assessment	
V. Conclusion	41
Resources	43

one: introduction

Policing Smarter Through IT: Lessons in Enterprise Implementation



I. Introduction

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 *Citizen and Law Enforcement Analysis and Reporting (CLEAR)*. 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

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.

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 the 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 the 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 departmental 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

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 of – and responsibility for – the final product. This section presents the issues and considerations encountered in building an IT system in a law enforcement environment.

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

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.

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.

*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.*

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 whom 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 have provided their expertise in developing the business logic coded into the software.

Knowledge transfer

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.

...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 with 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 a result of brainstorming sessions and system tests by experienced officers who 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. 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 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 are made. We occasionally saw deadlines imposed - perhaps out of frustration or as a management tactic - that everyone knew were impossible to meet. Deadlines that cannot be met have an effect on quality and reliability, and should be avoided.