Cisco Systems

Intelligent Government - The Next Wave

Network based transformation in **Policing**

Cisco Public Services Summit @ Nobel Week 2002

Contents

Introduction - The Many Challenges of 21st-Century Policing

Police forces around the world are faced with many common pressures. They experience strain upon resources, ever-intensifying critical public scrutiny, a blurring of the lines of jurisdiction between police and other criminal agencies—and a criminal world that is complex, pervasive, and increasingly sophisticated in its ability to mask criminal activity and the proceeds of crime.

Given this challenging environment, the police need to find ways to share information and resources more effectively, to engage with the communities that they serve, and to identify and restrict the opportunities for criminality which a world with greater mobility and fewer borders than ever before presents.

Underlying all these perceptions is the overriding concern that citizens express about public safety. Whether these concerns are related to real instances of criminality is not the issue, as crime figures in many countries have shown an historical decline. However, the perception remains that the public space is an increasingly dangerous one, and the custodians of law and order in that space—the police—are failing to provide the public with the reassurance that they seek.

In short, the challenges faced by the police in many countries around the world are formidable. Resources, as elsewhere in the public sector, are stretched, but the demands placed on the police are growing.

The organisational structures that police forces have typically used also work against the successful resolution of the problems that they face. Forces have worked in jurisdictional "silos," not only within their geographical borders, but also arising from the focus and function of the specific police work involved. Police involved in the detection and prevention of fraud, for example, will work in a separate unit to those who focus on robbery. Though the perpetrators of both types of offence may often be the same, it is quite likely that the separate divisions within one force will pursue intelligence as discrete entities, rarely collaborating or sharing the results of their enquiries.

The creation of an integrated national police force is predicated on the ability that the police have to effect a community of interest among all law enforcement agencies, and furthermore to extend the definition of that community out into the public arena.

The Internet and networking technologies are creating new means for the police to address and solve some of the issues that they face in the efficient execution of their various roles.

The power of the Internet and related networking technologies to fundamentally change the way that police work is carried out—and the delivery of police services to the public—is considerable. However, with a few notable exceptions, the police have failed to make full use of technologies that have the potential to help bring about these desired results.

Figure 1:
FBI website, public reporting page

Following the terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001, the FBI received more than 66,000 pieces of information from the public via its Web site (Figure 1). This overwhelming response demonstrates the power of the Internet to engage citizens in the process of combating crime.

Worldwide public concerns about security promoted by the terrorist attacks in the United States are to some extent echoed at a more local level with the present concern in many European countries about street crime. In France, for example, the media is daily full of headlines and lead stories which arguably contribute to an exaggerated fear of crime—a fear that the police are often seen as doing little to address. In the presidential elections in France earlier this year, crime was one of the major issues. Across western Europe, a fear of crime is pushing political debate and fuelling public demands for "something to be done."

One of the principal arguments rehearsed in the media, and in private, that advances the notion that the police are losing the battle against crime is the apparent lack of a visible police presence on the streets. Achieving higher visibility is one of the principal challenges that the police face, but their ability to achieve this is hampered by a lack of resources and conflicting priorities. Addressing the public demand for greater police visibility means finding ways to liberate operational police from the bureaucratic processes that keep them behind their desks and off the streets, away from the public domain. Technology that can help to liberate the police from desk-bound activities, while providing them with superior information-sharing capability and contact with centralised command structure is, and must be, a focus of planning and resources. The impact of wireless devices, capable of exchanging information (voice, data, and video) over a network of many different users and information sources, would considerably enhance police ability to operate effectively and maintain a highly visible presence. However, the stumbling block to achieving such systems resides not in the lack of available technology to implement such a wireless solution, but rather in the ability of police and political managers to create the organisational will within which such networks can be implemented. Where such obstacles have been overcome, the benefits perceived by both the public and operational police officers have been considerable.

The Networked Organisation - Technology and Culture

The ability to share information and collaborate is key to the success of many different types of organisation. In the private sector, businesses have invested substantially in the creation of networks that allow different parts of the business to exchange data, to work together from different locations around the world, and to ensure that the sum of knowledge held in an organisation is spread across and made available to as much of the business as possible.

The technological barriers to achieving this degree of networking capability are being eroded, as the development of increasingly flexible and agile solutions emerge that create the possibility for previously isolated and discrete elements of an organisation to communicate. Networks can encompass even the most mobile of organisations, with remote access and links as part of the technologically feasible, readily available solutions.

More problematic, though, is the creation of the organisation and business culture that allows such truly networked communities to develop. The police, for example, operate in clearly defined silos within forces, jurisdictional boundaries, and areas of functional responsibility. Breaking down the walls of those particular silos is a matter of changing the organisational culture and people's behaviour—not simply having the right technology available at the right price.

Many IT projects, however, are driven not by any underlying, shared vision of the desired outcomes of a new system in terms of benefits to workflow and process optimisation, but in terms of the IT itself. IT policies that are not strategically led with a focus on the benefits that the introduction of technology confers, and focus instead on a narrower agenda defined by IT functionality, are likely to founder and fail to be taken up within an organisation.

Leadership and a concerted effort to bring about cultural change are key elements of any successful networking strategy. Organisations that use IT successfully are not successful because they employ state-of-the-art technology—it is the manner in which they address their IT activities and incorporate them into their organisational aims. Leadership for such projects must come from the most senior levels, in order to create total organisational buy-in.

Information is the lifeblood of effective police work and a fundamental building block of the police's ability to provide public assurance. But information is only effective if it is available to the right person at the right time. The police do not suffer from a lack of information, but they often lack the means to put the information at their disposal to work effectively. An organisational framework that creates a clear picture of the information needs of every agency involved in fighting crime and delivering public safety is a prerequisite of any attempt to build a networked police community.

Managing the transition to a networked environment from one in which information has been guarded and collaboration has been rare is a significant challenge. The degree of change management involved is substantial. Without the public sponsorship of senior management, it is possible for middle management to maintain and prop up bureaucratic barriers that delay and frustrate plans to create enterprise-wide solutions.

The Drive for Better Policing

Public Opinion

The reporting—and misreporting— of crime has led to a widely held public perception that criminals are "winning,"—that the streets are less safe than they once were and that citizens are more vulnerable to crime against both their person and their property than ever before. Although this view is at odds with much of the research into trends and available crime statistics, public opinion and sentiment acts as a powerful stimulus to governments and, in turn, to the police.

Against this backdrop, police face the same spending restraints and the heightened expectations that confront other public-sector service providers. Inevitably, they must discover ways to do more with less.

Police forces in nearly all countries presently lack the ability to integrate their information and resources with other agencies and to communicate effectively with the public. This inability is not a result of a lack of technological solutions. Rather, institutional, organisational, and bureaucratic complexities and politics must shoulder the blame for much of the substantial lack of progress made by police forces to realise the potential improvements that the intelligent application of technology can provide.

The Paper Burden of Operational Policing

Much of the work carried out by police "on the ground" may be better categorised as policing behind a desk. A consistent complaint among operational officers is the size and complexity of the bureaucratic burden that they face.

A Day in the Life of a U.K. Policeman

On 16 May 2002, the Independent newspaper reported on a typical day in the life of a constable with the Metropolitan Police in London, PC Des Keeno. His description of the day illustrates many of the inefficiencies that face operational police officers:

- "Arrives half an hour early to work to read e-mails and other bulletins available from the network; have to arrive early because the system is so slow and complex."
- On arrest of suspect needs to process a case file, "which has to be handwritten. Name and address have to be written 30 times because the computer system is not integrated."
- Having worked an hour of overtime, able to claim 30 minutes overtime pay. "To claim must send three e-mails and obtain two authorisations."
- "Taking a prisoner into custody can take between two and eight hours. In extreme cases 40 separate forms have to be completed by officers and civilian colleagues for the arrest of a single shoplifter."

Many presently available applications could help the police to speed up their reporting and administrative obligations without comprising the safeguards that existing systems are designed to deliver. As an example, Wiltshire police force in the U.K. has begun a programme of creating electronic versions of paper forms. The time and revenue savings that they have gained amount to the equivalent of deploying seven full-time officers, and they have made considerable gains in efficiency. Where previously 85 percent of paper forms were rejected because of errors, their electronic counterparts have eradicated all error-generated rejections.

The London Police Service in Ontario, Canada is part of a criminal justice system that has taken a progressive approach to the implementation of communications and information technology. Police officers are equipped with robust mobile workstations held in specially designed cradles in patrol cars. Integrated voice and data transmissions are linked to headquarters, so that officers on patrol can be sent incident details directly for a computer-aided despatch (CAD) centre and, relay information back to the centre for processing.

When an emergency call is received at the call centre, the CAD system automatically sends details of the caller to available officers via their mobile workstation. Officers can complete incident reports while on patrol, and if an arrest is made, this information is automatically used to complete cell-booking forms, and to produce a brief for crown prosecutors and defence lawyers. Other forms can also be completed using the information submitted by the arresting officer—and none of this process requires him to return to the police station.

The system is also able to make information available to the media—it automatically provides information about selected incidents to a media Web site, to which members of the press holding the appropriate passwords can gain access.

Assessing Progress - Theory vs. Practice

Many of the problems and challenges that police face on an operational level can be addressed successfully through the strategic application of selected technologies. Networking technology provides the police with the potential to achieve better communication, to engage the public more effectively, and, through the use of wireless solutions, to liberate the desk-bound operational police officer.

However, the availability of the technology is less of a constraint than the bureaucratic and organisational barriers that represent a far greater barrier to change. In the U.K., for example, several different bodies are responsible for examining the possibilities that new technology can offer to the police force. The political difficulties that such an uncoordinated approach creates are self-evident. In other European nations, the police are similarly fragmented. Though they share a common goal of fighting crime, their development as independent forces has, to date, hampered attempts to bring them together under a cohesive strategy for implementing solutions on a national, or even international, basis.

The U.K. Home Office-sponsored report by Superintendent Peter Woods of the Northumbria Police outlines the present shortcomings of online provision by police in the U.K.: "I contend that 43 versions of what the police in England and Wales have to offer over the Internet is not what the public want, although it may be what some police forces think that they want. There is a need I believe, for a national police online service, so that wherever a citizen is he or she can expect a consistent high quality service and a similar menu of service options offered. There are significant ongoing cost-savings available in having a standard service provision that enables data to be shared between forces. Using a national online police model, services will be offered in one, not 43 different and incompatible ways.

The public, many of whom do not know which force area they are in, do not want to chase around a www.police.co.uk Web site looking for their home force, only to find that their local police does not offer a particular service that they want to use, while neighbouring force offers it all. The Government's attempt at providing a national service – reporting a minor incident online – is a start, but nothing like the comprehensive service I propose.

The current delivery of online police services is a mess that will get even messier if the police service nationally is not taken back to basics. The simple questions: 'What does the public want and how is it possible to deliver?' need to be asked and the cost efficiencies of providing many police services online, some of dubious quality, need to be considered before the situation is allowed to develop any further on an ad hoc basis. From the human rights point of view, why should it be that five months or even five years down the line a person living in one police force area, can access twice as many police services online as a person in another police service area? It's simply not compatible with human rights legislation and is not tenable in the long term.

Any new vision for the national online police service of the future should herald the end of the police service as a fortress, where all information is guarded and ways into the police organisation are strictly controlled. It should be the beginning of the police service as a transparent organisation. So that people can come and go and pick and choose what service they use, and how they use them, in all but the most sensitive of police functions."

Moving towards Web- and network-based solutions for the police are not in themselves likely to effect a change either in public perception or the delivery of services to the public. Initiatives, in which IT is the driver rather than serving the strategic imperative being pursued, are likely to founder and fail to deliver expected improvements.

The serious issues that police in all parts of the world face will not be resolved by the adoption of IT alone. Though there are undoubtedly many technological innovations that will assist police to make better use of resources and to collaborate, share information, and operate more effectively, these must be applied in the context of a reassessment of organisational priorities and behaviour designed to promote and maximise sharing and openness. The business case for change must inform the IT policy.

The Possibilities of Networking

Unlocking the Power of Organisational Information

Communities are infinitely more powerful than many separate individuals working in isolation. Networked information technology has the potential to unlock the latent abilities of isolated and discrete members of an organisation to pool resources and to collaborate effectively, regardless of geographic location. Knowledge that is held within an organisation is its most valuable resource, but its true value can only be realised when this knowledge is made available and spread throughout a community. For police forces to achieve this, a fundamental change in culture is required.

Superintendent Peter Woods of the Northumbria Police Force says in his report on electronic policing: "The police service, like many large private and public-sector organisations, has within it a huge amount of information. Much of the nonsensitive data would be useful to the public, but is not readily available to them unless they call in at a police station or speak to a police officer in person. An online police service available 24 hours a day, via any Internet-capable device, could go a long way to making information more accessible and therefore useful to the citizen.

Much information within the police service is currently in the heads of specially trained police officers and support staff who have built up their knowledge over a number of years. Front-line policing is normally carried out by staff who are the least experienced, or are in training themselves. Our most experienced staff only have the opportunity to use their specialist skills when called upon to do so. So a few people only experience the benefit of their knowledge. Through the Internet, the police could, for instance, announce that an officer with experience in crime reduction will be available to answer any questions online at a certain time and date. Large and small businesses, town centre managers, local authority staff, and others would have access to this officer's expertise and thus have their questions answered live online or offline at a later date."

Sharing Law Enforcement Information with the Public: The U.S. National Instant Check System for Firearms Dealers

Firearms dealers in the United States are obliged to check the background of any member of the public who wishes to purchase a gun. The National Instant Check System (NICS) gives them access to FBI databases that allow them to query whether the sale of a firearm to a particular individual would constitute an offence. Over 100,000 licensed dealers in the United States query the system. Dealers make a telephone call or send an electronic message to the NICS centres and receive an immediate response. Though details about the would-be gun purchaser are not revealed, the requests are checked against a comprehensive list of excluding conditions. The NICS system is the only justice records system in the U.S. that shares information directly with the public.

E-Learning

Sharing information and knowledge in the context of the networked environment means creating the possibility for all existing users and new users (such as the public and law enforcement and criminal justice agencies) to learn.

One of the most powerful applications of the Internet is e-learning. E-learning applications create a learner-driven experience, where knowledge resources can be used and information found by the user in the time that he or she has available. For the police, the potential of e-learning is extremely powerful.

E-learning looks outside the traditional classroom-based training to deliver education and training where and when it is needed. E-learning techniques bridge the gap between learning and implementation of acquired knowledge. Because e-learning is needs-based and user-driven, training does not have to fit around a schedule—the learner is able to dictate the pace and the location of learning. Training is focused on the individual's unique requirements.

The Queensland Police Service (QPS) in Australia adopted an e-learning programme in 1996, and since then has rolled out the programme on a statewide basis, with materials and content now delivered online (Figure 2). The size of the territory that the QPS has to cover and the dispersal of personnel across that territory mean that traditional learning methods present a number of practical difficulties.

Catherine Sparks, Coordinator of Learning Services with the QPS explains: "The geographically dispersed nature of the QPS and the large number of people needing training in a short period of time presented major problems with the traditional classroom-based training method. The issues that we had to consider in devising a training programme included the wide training needs and abilities in the QPS and the need for consistency of training and assessment.

There is an ongoing need for training and refresher courses in QPS. The issue of rapidly distributing timely information with respect to legislation changes and new procedures is increasingly being addressed by e-learning materials. The delays and overhead of cascading seminars, printing, and distributing updates and revisions are avoided."

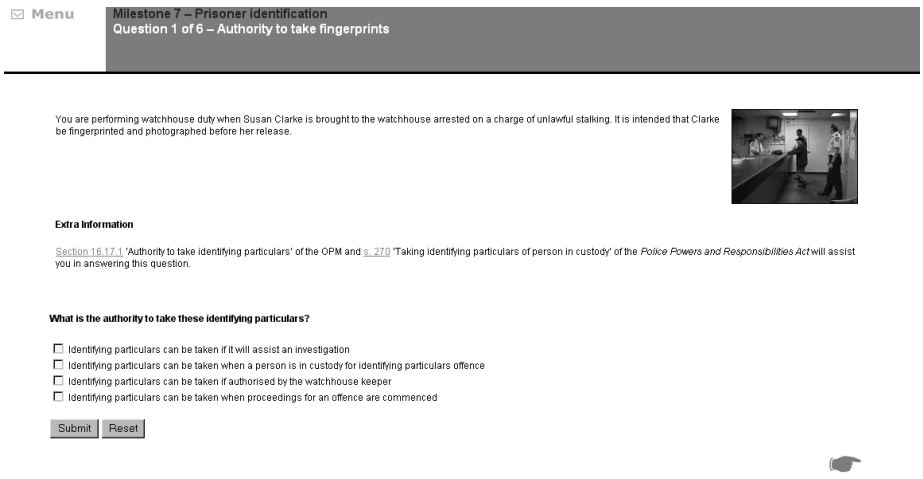

Figure 2:
A Module from the Queensland Police E-Learning Suite

Other forces around the world are also adopting e-learning techniques. In Italy, a major e-learning initiative for members of the national Carabinieri force is underway, with basic IT skills, language courses, and training and updates on procedures being delivered over a networked e-learning platform. The postal police that have been assigned responsibility for combating Internet crime in Italy have access to the Cisco Networking Academy™ Programme—the most successful e-learning programme in the world.

The Hong Kong police force has also embarked on an e-learning programme, including highly interactive and simulations-based content that allows users to inspect a crime scene and gather evidence.

Illinois police have integrated an e-leaning solution into their recently developed criminal justice system, the Law Enforcement Agencies Data Systems (LEADS). E-learning here is provided as a desktop application, giving both police and other workers in the criminal-justice system desktop access to instruction on how to use the new system. Users must complete the appropriate training modules before they are able to use a specific element of the system. Because the learning application is integrated into the package, users' progress can be tracked and access to elements of the LEADS system automatically granted only when particular training modules have been completed.

Using Networks to Enhance Public Safety

The use of the Internet and networks in many different aspects of life is due to expand significantly over time. The range of devices with the ability to access different networks, both public and private, is constantly increasing, with the expansion of bandwidth and advances in the processing capacity of mobile telephones and PDAs creating new possibilities. The ability to provide mobile personnel with access to data has profound implications for policing. "Always on, always with me" devices such as Internet-enabled mobile phones and PDAs are likely to become an increasingly common part of the modern crime fighter's standard equipment.

The value of connectivity is, of course, derived from what the user is connected to. One example that dramatically illustrates the power of mobile access is the wireless IP surveillance solution being used in the City of Seal Beach, California. The system links patrol officers to live video feeds from a range of commercial and public institutions.

The system, developed by Loronix Information Systems and Cisco Systems, is being piloted with links to the video surveillance systems in bank branches in the Seal Beach area. Police officers can view real-time video of an incident in progress on laptops installed in patrol cars. Eventually, the system will be made available to specially equipped PDAs.

When a bank employee triggers an alarm, the bank's existing video system relays images, via a secure network, to both the central police station and patrol cars. Michael Sellers, Chief of Police for the City of Seal Beach, describes the benefits: "It's like giving our officers remote, real-time x-ray vision. Instead of waiting until after the crime takes place and there are victims, we can see video of the crime actually taking place, allowing us to make better, fairer decisions."

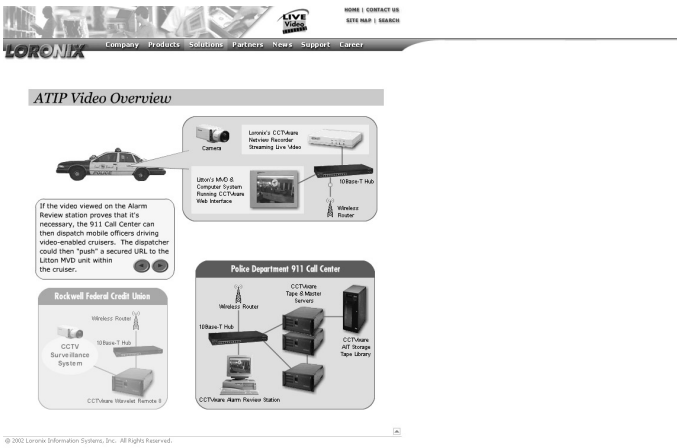

Figure 3:
Loronix website showing the overview of the video system as used by the Police for the City of Seal Beach

Because the system greatly enhances the immediate intelligence-gathering ability of a mobile police force, resources can be deployed appropriately to respond to a specific event. Real-time video links also mean that suspect identification can be made with greater speed and accuracy.

Implementation of the system has also proven to be cost-effective. The system uses existing video surveillance equipment, and operates over a number of connected local-area networks (LANs), rather than requiring more expensive installation of wide-area networks (WANs) (see figure 3).

Police in Singapore are testing equipment that is designed to give them access to central databases on the move, without the need to tie up resources in call centres or operations rooms. Police will use customised PDAs allowing wireless access to databases of stolen cars and criminal records. The system is also being designed to offer access to photo libraries of missing persons, and for crime scenes to be beamed live to a police officer "on the beat."

Such innovations will help to free up police time and push resources back into the public space, where demand is at its most acute. However, the information infrastructures that underpin the use of mobile devices must be in place. Various commentators have expressed their concern that the use of mobile devices can be employed as window dressing, masking the weaknesses and gaps in the information systems that power the use of mobile data access.

Engaging Directly with Citizens

Using the Internet to provide the public with information and a limited number of interactive services has been adopted by a growing number of police forces around the world. Citizens in Chicago, Illinois, for example, are able to identify crime hotspots in their local neighbourhood by tapping in their address to the Citizen ICAM Web site (Figure 4). The site then displays a map showing the incidences and types of crimes committed in a given time frame. Citizens are also able to e-mail the police with information about crime.

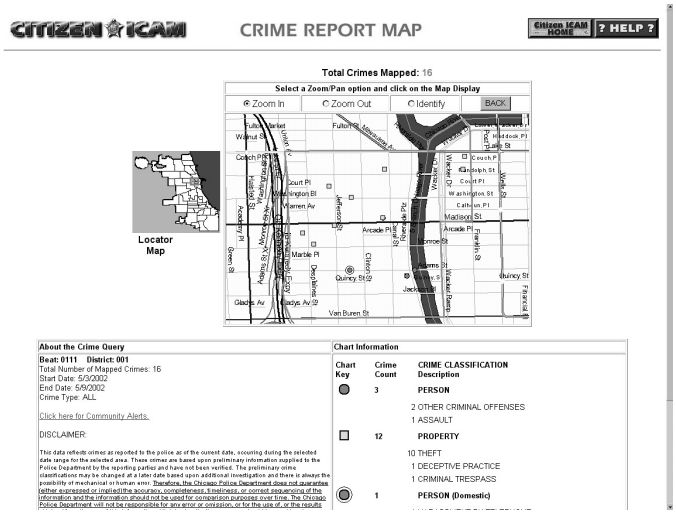

Figure 4:
Citizen ICAM

In a recent development in the U.K., the Police Information Technology Organisation (PITO) has launched one of the first national initiatives, allowing the public to notify police of minor crimes. The National Online Reporting system allows citizens to enter the details of minor, nonviolent crimes of which they had either been victim of or witness to. The Home Office study into the role of police visibility and public reassurance, "Open All Hours," was critical of the service because it failed to create an integrated national crime reporting capability: "The application could initially only be online notification of crime, rather than full report, for a number of reasons:

The variation in crime reporting systems meant that the information supplied had to be at the level of lowest common denominator. Following notification of a crime, forces have to contact informants for fuller details, and to supply the crime reference numbers required for insurance purposes.

- Short timescale prevented development of interfaces to different crime systems in use
- Absence of secure networks prevented forces from electronically transmitting information within their force or to another force
- As the project had not arisen from strategic development, forces were in different stages of readiness to adopt the process and integrate it with their systems
- The complexity of the front-end application, even for simple notification, was considerable

An apparently simple idea of allowing the public an additional access point to report crime to any force resulted in a system that added layers of complexity to the process. Instead of a full crime report, forces were faced with a notification that they had to print off, send to the appropriate district or division by fax, and then manually input again, after contacting the informant for further information.

Development of future national e-services will be severely hampered unless a suitable migration strategy for all forces is considered at an early enough stage."

While information is being made available, and there are attempts to provide public service through more accessible channels such as the Internet, the absence of a fully integrated strategy for service delivery will retard any efforts to create genuinely national and joined-up solutions. But in suffering from a lack of coordination, the U.K. is by no means alone.

Networked Policing in Action - Operation Crackdown

Operation Crackdown is a project by Sussex Police in the U.K. to tackle the problem of abandoned vehicles. As the price of scrap metal has fallen substantially—driven down by European legislation that creates new guidelines for the environmentally safe disposal of old vehicles—so the willingness of scrap-metal merchants to collect cars that have reached the end of their useful life has declined to the point where they now make a charge for collection instead of the fee that owners have been able to charge in the past. Many more unwanted cars are now abandoned by their owners, who are unwilling or unable to pay the fee for the car to be removed. Abandoned cars contribute to an atmosphere of neglect, attracting vandalism and arson. Nationally in the U.K., the costs incurred for removing abandoned vehicles stretches to over half a billion pounds.

Operation Crackdown aims to use networking technology to cut the time any vehicle remains abandoned from an average of 28 days to just 48 hours. The system for removing cars relies on more than one stakeholder, including the driver and vehicle licensing authority, the police, the local authority, the fire brigade, and the removal agencies. In order to expedite the process of vehicle removal, police powers will be enhanced to allow them to sanction the removal of an abandoned vehicle. A Web-based vehicle information hub will hold records of abandoned vehicles. Additionally, members of the public will be able to log details of a vehicle that they believe has been abandoned, giving precise details of the vehicle's location and condition. The information hub will be accessible via police intranets and various other stakeholder extranets, but it will also be made available wirelessly to police with mobile-enabled PDAs. These will be able to share information with the central data hub, and will allow digital images to be uploaded. Forms can be completed at the site rather than back at the station, saving substantial time and effort.

Some of the technical challenges raised in the Operation Crackdown pilot have clear parallels in other areas of policing. The development of reliable and secure wireless access is clearly a key determinant of the ability that the police will enjoy in rolling out similar solutions to other areas of activity. One of the key technologies that the Operation Crackdown project utilises is the ability to send repurposed information from a central database to various different devices and over a range of different platforms. The Cisco Content Transformation Engine (CTE) allows files to be created in a format that can be read and exchanged with the central server. Given that one of the principal benefits sought by the police in their use of technology is a substantial reduction in the amount of paperwork that is generated, the widespread adoption of tools such as the Cisco CTE solution in place for Operation Crackdown can only help to move the police towards that goal.

Call-Centre Technology

Learning from Best Practice

The interface between the public and the police is crucial. The complexity of the decisions that have to be made and the demands on call-centre operatives are considerable. It is not surprising that the traditional telephone systems used by the police have not always been able to keep up with the demands placed on them and have sometimes been seen to fail in their basic task of allocating police resources efficiently to a variety of situations.

The information that the police receive through a call centre is considerable and diverse. Requests for information and the need to distinguish between urgent and nonurgent requests for assistance means that telephone operators must be able to distinguish and discriminate between any number of calls in order to ensure that resources are deployed effectively.

A study carried out by MBA students at Manchester Business School in April 2001 examined police call-handling performance in the U.K. One its findings indicated that the sheer volume of calls—undifferentiated between urgent and nonurgent, internal and external—effectively "swamped" switchboard operators, who had few alternative means of delaying with calls and thus managing the flow of information more effectively: "In many forces, significant additional call-handling loads came through switchboard represents, internal calls through the switchboard, lack of voice-mail facilities, lack of 'help-desk' facilities, and, significantly, lack of alternative means of communication—in particular e-mail."

More effective call-handling capability is a crucial next step for police to make. The report found that where forces had installed updated technology, there were significant improvements in the force's ability to direct call flow more effectively: "Where forces had invested in the latest call-centre technologies, this was perceived to have led to greater integration of process and systems with concurrent reduced manning, increased opportunities for civilianisation, and greater flexibility. At the same time, the use of these technologies emphasised the potential for the realisation of scale opportunities."

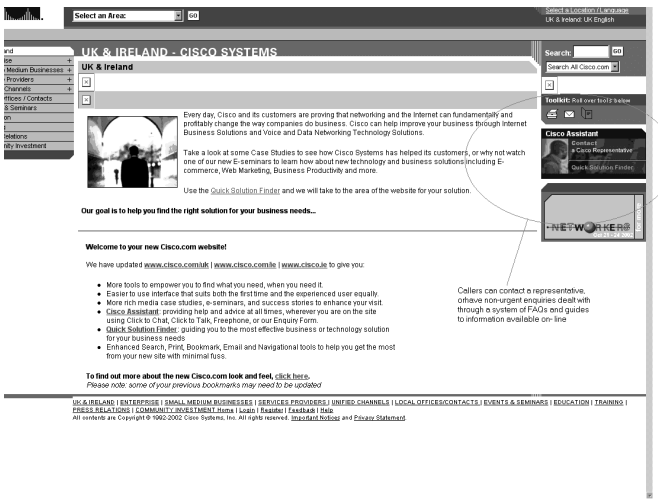

Figure 5:
Cisco Call Assistant—Managing Information Flow Online

Moving Toward Real-Time Information Sharing

The National Institute of Justice (NIJ) in the United States has been working toward creating a programme to help law enforcement and other emergency services to create interoperable communications systems. Communications interoperability is a vital next step in creating a more effective and efficient police response. Interoperability means allowing individuals and teams to hear and "listen in" to everything happening around them. It allows dispatchers to send multiple units to the scene of an emergency quickly, and it allows the first police officer to arrive at the scene of an incident to communicate with any and all units.

Public-safety communications in the United States exhibit the same problems and limitations as they do elsewhere in the world. Namely:

- Governance of the system is widely distributed and diffuse
- Equipment used by some forces is incompatible with that used by others
- The infrastructure is aging and needs replacing
- A small number of specialists supply the market, restricting the market

The problems and obstacles to be surmounted in order to change present provision also hold true for countries beyond the United States:

- Replacing the existing infrastructure will require a substantial capital investment
- There is a lack of flexibility in terms of the technology and systems that can be deployed
- Annual maintenance costs are high
- There is a need to "over-engineer" the system in order to create operational safeguards
- The planning and implementation cycles are long
- Mistakes made at the planning stage can cause serious problems later
- The law-enforcement culture is risk-averse and reluctant to change

Despite these formidable barriers, there remains a pressing need to bring about a far more integrated means of communicating than is presently available. The Agile programme in the United States aims to provide the direction and governance for local and state public-safety agencies to communicate across both agency and jurisdictional boundaries. Under the Agile programme, 17 public-safety organisations, along with the National Task Force on Interoperability, are involved in developing research and guidance that will allow emergency services to build more integrated communications solutions. The Agile programme has a number of trial projects in operation and is testing equipment that allows previously noncommunicating devices to work with one another. Agile's ACU-1000 Switch operates by effectively "translating" the signal from one device so that it can be received and understood by up to 12 incompatible radios. The equipment is presently undergoing evaluation in the field in more than 50 sites across the United States.

Keys to Effective Information-Sharing System Implementation

In a presentation to assembled European delegates in June 2002 at a conference in Madrid aiming to explore the interoperability of European systems, Glenn Schmidt, the Director of the NIJ, outlined some of the key elements of success that the agency's work has highlighted.

The NIJ acts as an "honest broker" between law enforcement agencies. As it has no operational role itself, it is able to mediate between other agencies without having to defend a particular territory or jurisdiction. The NIJ has a standard-setting role that allows it to evaluate and assess, on behalf of other agencies, the technologies and systems that may be deployed by any of them. It also acts as a pioneer of new techniques and technologies, helping to build and reinforce credibility for new systems.

Schmidt identifies the following elements for building projects that will create effective inter- and intra-agency data sharing:

- Fund development of new tools and technology after needs have been identified
- Leadership at all levels is crucial:
- National and regional leadership
- Committed users
- Leadership to ensure that all involved in the development and use of the system feel that they have a stake in its eventual success
- Provide funding in a systematic way from a few agencies. This avoids duplication, creates economies of scale, and recognises that no single agency will be able to fund and deliver a project on its own.
- Fund the development of multiple approaches at first and avoid investing in the overarching, "big-fix" solution too soon. Allow for iterative development.
- Make the most of existing technology wherever possible.
- Ensure that funding is not restricted to research and development, but is made available for training, maintenance, and upgrades.
- Continue to promote the new system after it becomes live, and ensure that reliance on the old system is curtailed as swiftly as possible.
- Encourage the continual participation in the governance of the system by all stakeholders at all levels

Network-Centric Warfare - A Model for 21st-Century Policing?

In his book, Understanding Information Age Warfare, David S. Alberts writes:

"As we begin the 21st century, we have an opportunity to step back and consider fundamental changes in the way we invest in, acquire, equip, and train our forces. The dynamics of the Information Age will punish us if we do not adapt to a new way of doing business… we must be prepared to endure disruptive change."

Network-centric computing—the move away from platform-based IT solutions—has been made possible by advances in IT that have allowed different operating systems to communicate. Network-centric computing is transforming business because it creates the opportunity for far-wider collaboration among an infinitely richer mix of users than has been possible before. In the public sector, its impact will become increasingly evident as governments pursue strategies to move many services and interactions with citizens into an online environment. However, there is one arena in which the transformational impact of networking is already clear—the military.

The emergence of network-centric warfare clearly illustrates the potential power of networking to transform the performance of an organisation. In a report to the U.S. Congress made in July 2001, the U.S. Department of Defence described how the adoption of network-centric thinking has the potential to utterly and radically reshape the military—and specifically the combat—arena: "Network-centric warfare is the military response to both the challenges and the opportunities created by the information age. The term 'network-centric operations' provides useful shorthand for describing a broad class of approaches to military operations that are enabled by the networking of the force. When these military operations take place in the context of warfare, the term network-centric warfare is applicable. Network-centric operations provide a force with access to a new, previously unreachable region of the information domain. The ability to operate in this region provides war fighters with a new type of information advantage. This advantage is enabled by the dramatic improvements in information sharing made possible by networking. With this information advantage, a war-fighting force can achieve dramatically improved shared situational awareness and knowledge."

The comparison with the police is salient on several levels. The police are engaged in a "war" against crime, and are increasingly focused on intelligence-led methods of crime detection and prevention. Operational policing, like warfare, involves communication between mobile operatives, who need to share information both between themselves as well as with centralised command centres responsible for providing the strategic framework within which operations should take place.

The conclusion to the Department of Defence's report to the U.S. Congress summarises the challenges that the military needs to overcome in order to see network-centric concepts implemented. These steps apply equally well to the police.

Network-centric capabilities:

- Involve new ways of thinking about how tasks and missions can be accomplished.
- Change organisational roles and responsibilities.
- Require that information be shared outside of existing communities.
- Depend, in part, on the development of new technologies.
- Require a better understanding of how to create, share, and exploit awareness.

To make network-centric warfare a reality requires:

- An infrastructure that is robustly networked to support information sharing and collaboration.
- A climate that fosters disruptive innovation.
- An appropriate technology base and an improved understanding of related issues.
- A way of analysing and assessing network-centric capabilities.

"We've really got to start modernising every single action that is taken by the police."

David Blunkett, Home Secretary, United Kingdom

Summary

As this paper shows, police forces around the world face a series of considerable challenges. Technology, and networking technology in particular, can be used to address many of these challenges. However, networking technology can only be implemented effectively in those organisations that are ready and able to embrace the often profound changes that its introduction is likely to create.

Better use of existing resources alongside techniological innovation is key to achieving systems and organisations that can deliver real and measurable enhancements of public safety. Projects to modernise policing must be governed by the business case and not driven by the technology that will help to create them. It is vital therefore, that means of measuring project effectiveness are created and adopted across an entire force. To manage a problem (and its solution) it is vital to measure the problem (and the impact of the solution).

Many of the most powerful solutions that have been implemented in various countries have not relied on state of the art technology, but have instead used existing equipment or systems in new ways to powerful effect – to make it possible for communication to take place between previously isolated elements of an organisation. The use of mobile and wireless technologies (many of them already plentiful and cheap), for example, will become increasingly standard issue for policemen and women on the beat to connect them to data and video allowing them to police with transformed intelligence capabilities.

Though specific technologies may help the individual police officer to perform more efficiently, the real power of networks resides in their ability is to assist forces and departments to collaborate and act together in pursuit of the common goal to enhance public safety. But to achieve this goal will require more than the right technology: political will and an enterprise-wide willingness to embrace the disruption that such efforts to achieve communality of action as well as purpose will create are essential for the creation of more effective, responsive and intelligence-led police forces.

Series Editor Simon Willis

Internet Business Solutions Group EMEA

Cisco Systems

Enquiries swillis@cisco.com

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the U.K

11/02
nobel/policing