CGI

Experience the commitment®

WHITE PAPER

Tomorrow's Force

How technology can help the police evolve to support a changing society

With resources strained as far as they can go, police forces recognize the need to shift from traditional, reactive policing to a more proactive model. This means changing processes and adopting new technology so an officer's time can be focused on tasks with the greatest impact. This white paper reviews some of the new ways police forces are working, as well as the technologies that are helping to advance those processes.

June 2014

Contents

Today's dilemma

Today's police forces are facing something of a dilemma. Their fundamental role in society has not changed; they must enforce the law and protect citizens as they always have done. However, the environment in which they operate looks nothing like it did 20 or even 10 years ago.

A local crime may no longer be masterminded locally but organized thousands of miles away across computer networks in different jurisdictions. Cheap technology and the unregulated growth of the web have opened up lucrative channels for criminals, leaving citizens vulnerable to cybercrime and the police struggling to keep up.

Citizens' expectations have also been driven up by the prevailing wind of accountability and discussion around high-profile cases in the media. Add to the mix the enduring taste for TV drama where every crime is solved, and the result can lead to police under pressure to secure more prosecutions.

At the same time, the police increasingly are expected to deal with a wider range of complaints such as a low-level dispute with a neighbor or a nuisance dog. Citizens want everything on demand, including their law enforcement, but tighter budgets mean that having a police officer on every street corner is no longer a viable option. This is particularly true as the need for a virtual police force to fight cybercrime is becoming more urgent.

The long-held "get the job done" attitude of the police has meant that they have responded to this change admirably by doing all they can to adapt and stretch resources to meet the need. But the pace of change demands a new approach.

Police forces throughout the world have realized that resources are strained as far as they can go, and that only by shifting the emphasis from traditional, reactive policing—solving crimes after they have happened—to a proactive, prevention agenda, can they meet these new challenges head on.

PURSUING FRESH OPPORTUNITIES

A more proactive model requires changing processes and adopting new technology to focus a police officer's time on tasks that have the greatest impact. This can be achieved in five key areas:

- **Informed prevention.** A more systematic approach to gathering and analyzing data that reveals trends in criminal activity will lead to a more effective use of resources to target crime and prevent it from happening.
- **Multi-agency working.** By working closely with other agencies, the police will be able to catch criminals quickly, respond to serious incidents in a joined-up way and to find new methods of protecting people who are at risk of crime.
- **Taking it mobile.** Tomorrow's police force needs to be fully informed when out in the field with more widespread use of secure personal mobile devices. Mobile working will also reduce the need for officers to return to the office to write up a case.
- **Citizen-led policing.** The force will need to engage with its citizens using social media and other technology to help the public become the extended arm of the law by gathering evidence and stopping criminals in their tracks.
- **Fighting cybercrime.** Tomorrow's force must be ready to address cybercrime head on, warning citizens of behaviors or sites to avoid and tracking new behaviors and criminals across the web.

This reality of policing on a smaller budget will not be short-lived; it will become the new normal.

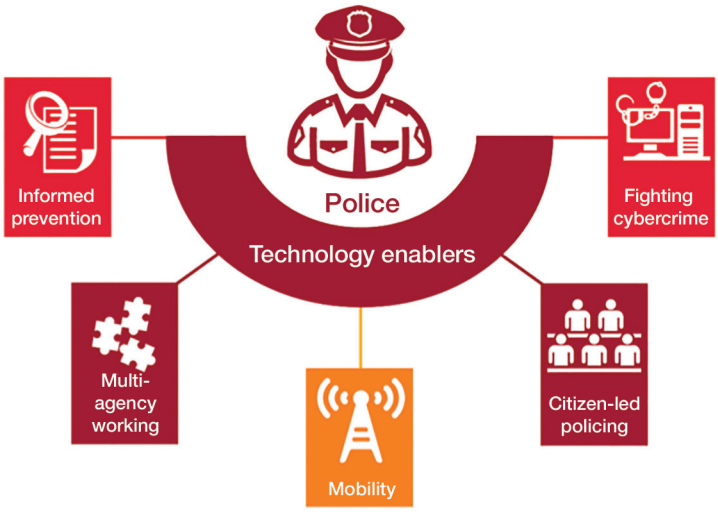
The police mission in the twenty-first century: rebalancing the role of the first public service

Reform, April 2014

Reform (reform.co.uk) is an independent, non-party think tank whose mission is to set out a better way to deliver public services and economic prosperity.

As this white paper reveals, these new ways of working and the technology that supports them are not the far off dreams of ivory-tower academics. They are already being introduced across different forces today, helping police manage their budget cuts successfully, while reducing the time it takes to gather evidence and solve more crime.

Tomorrow's police force



Informed prevention

There remains a pressing need to close the gap between citizens' expectations of crime prevention and the reality of it. To meet this need, technology and work processes must be refocused around information and intelligence-led policing to help prevent crime.

This can be achieved through:

- Analyzing data on criminal activity at a local level
- Harnessing the power of big data
- Monitoring social networks and using these channels to create a dialogue
- Making predictions based on patterns of activity and behavior
- Automating analysis of digital data on mobile and other devices.

ANALYZING LOCAL DATA

A local police force armed with an effective management information system will be able to reveal not only the crime hot spots but also the types of crimes committed in those areas at certain times of the year, month or even day.

Equipped with this information, police forces can deploy only the personnel needed in the right places and at the right times, making much more effective use of resources. This can have a significant impact on reducing crime in a short space of time.

HARNESSING BIG DATA

Opportunities for crime prevention are more abundant in our connected society, and there are many data streams which the police can pursue to prevent crime from taking place. The use of big data analysis provides huge opportunities for police by drawing out patterns of activity that may be suspicious.

MONITORING SOCIAL NETWORKS

Monitoring the chatter on social networks identifies the little signals among all of the noise that can give an early indication of trouble. Technology can help make sense of this social "noise" and point police in the direction of potential issues.

For example, tweets might reveal the violent intentions of a group of football fans at an away game in a certain city. The police could then react with more presence at the venue to identify known troublemakers. In some cases, the police may need only respond using the same social media channels to dampen the fire by sending an immediate message to the virtual community that it is being watched.

IDENTIFYING PATTERNS

Another approach focuses on preventing crime among known individual criminals or gangs. By honing in on a geographic region or group of people, the analytics are done on a very specific set of data around their movements. Previous criminal activity by a group or individual is examined in order to establish with reasonable accuracy the likelihood of what will happen next on the basis that patterns emerge. The historical data effectively provides an early warning system of future activity.

Lessons in targeted prevention

A regional police force in Northern Europe analyzed a demographic of people recently released from prison and noted that they were most likely to reoffend in the same type of crime within a certain timeframe. The police monitored them closely at this dangerous time and engaged with them through social services to prevent them from reoffending.

AUTOMATING DIGITAL DETECTION

There is further opportunity to make processes more effective and reduce the time it takes to analyze digital data by automating it. With improvements in facial recognition and automatic voice transcription continuing apace, substantial efficiency gains can be made to allow staff to solve more crimes. Today, if a force is equipped with the right data scanning technology, police officers themselves can scan the data using mobile phones, tablets and laptops to uncover evidence quickly rather than waiting two or three months to have those devices analyzed by specialist officers.

As an example, if 40 mobile phones were recovered during an investigation, they could be plugged in to the scanning system and a copy of all data—including names, phone numbers, email addresses and other pieces of vital information—would be available from historical texts, emails and applications.

This data could be cross-referenced with geospatial data so the police can know where the phones have been. From this information an investigator could say, "There are six devices in that batch that have relevant information and I'll use those six to build my case." The officer would get the basic data needed quickly to help investigate the crime, and analysts' time would become more efficient as they would only be sent the relevant phones to be analyzed in detail.

The technology can also make links between the data to tell investigators how often a name appears on certain devices, for example. So if someone denies knowing a suspect, the evidence is immediately available from his or her phone.

This information can now be gathered at the push of a button, rather than from the creation of complex spreadsheets, and ensures police officers are more effective.

Data analytics allow police forces to:

- Predict crime hot spots
- Monitor social media for potential trouble
- Track social media activity of known criminals for clues to past or planned crimes
- Save time in analyzing the electronic devices of criminals.

Getting early warnings

In 2011, the Philadelphia Police Department was caught off guard by a series of flash mob incidents involving a significant number of youths, resulting in shoplifting and a series of assaults. The police department later learned that the youths had been publicly posting their plans for days before the incidents, but the department was not routinely viewing social media sites. This quickly changed. The police department currently reviews public postings on Facebook, Twitter and other social media to learn in advance about potentially dangerous incidents.

CGI

Integrating emergency services

In the Netherlands, where the 24 regional police forces are undergoing centralization, the 24 control rooms are now being shifted to just 10 locations and this has led to a rethinking of existing processes.

Currently, when a Dutch citizen phones the emergency number, they are asked, "Who do you want: police, fire or ambulance?" Most of the time, this is quite straightforward; however, there are cases where more than one service is required, or callers themselves are not sure of the need, they just want help and want it quickly.

So, the control rooms are now considering asking the question, "How can we help you?" so that they can organize the right people to deal with the incident. Then, all the services involved have the same information from the start.

It is a simple shift of focus that will have a huge impact on getting the right resources to the most serious incidents instantly.

Multi-agency working

An important catalyst in the shift to more proactive policing is the rise in multi-agency working. This practice is helping police more effectively solve crime and in many cases prevent it from happening in the first place.

Multi-agency working will be aided in the future by predictive modeling which will allow police to accurately identify high-risk situations where additional scrutiny should be applied. Examples include situations with the potential for domestic violence or child abuse.

Lessons from a tragedy

In 2013, a serious case review was conducted in the UK around the handling of the murder of Daniel Pelka, a four-year-old boy who was abused and starved by his mother and her partner. In Daniel's case and others like it, the various entities involved—such as police, social services, schools and the health trust—did not come together to analyze the case until something had gone wrong and it was already too late.

Cases such as Daniel's highlight inconsistencies in record keeping, silos of data held in different systems across agencies, under-resourced individuals and a lack of cooperation across agencies. The information that was necessary to make life-saving decisions was either sadly lacking or just had not been shared. As a result, the UK has begun piloting Multi-Agency Safeguarding Hubs, or MASHs, to promote better communication between relevant agencies so that essential information is available to help professionals make the right decisions at the right time.

There are around 30 regional MASHs currently working in the UK. Although there is effective prevention work as a result, many MASH teams are swamped with a backlog of cases. Much information is searched manually and the sharing of data is time-consuming. Data is often warehoused, so can be out of date and often is available only for the very serious cases being highlighted. Enabling escalation of the less serious cases is still a future vision.

Technology can help MASH and other multi-agency hubs by making data accessible in real time by those authorized to view it, so that action can be taken swiftly by the professionals involved.

This means that if the police are called to a domestic abuse incident, they could access information using their secure mobile device to learn, for example, that social services are already involved in the welfare of the children and there is a history of abuse with one parent.

Currently when the police turn up at any address they will be unaware if there are any children in the house at all unless they ask at the scene. Information could inform the police's response to this situation to ensure the safety and welfare of the victim.

This information could even be identified at the initial call and presented to the operator such as:

- The number of times the residents have called in the past
- If there is a firearms license attached to the address
- Whether the household is known to the local authority
- If a member of the household is a subject of intelligence or has a criminal record
- Whether there are children living at the address.

Such knowledge increases the opportunity for collaborative working across agencies as well as timely intervention.

FORMING PARTNERSHIPS

Multi-agency working makes sense, as there is no longer one single agency responsible for protecting the public. Justice organizations and other entities such as health authorities, fire departments and education services are involved. Volunteer organizations and the legal profession also have roles to play.

Cooperation between organizations and individuals from different domains can be much more fluid as technology enables a review of the processes behind multi-agency working.

One example is the Police National Database in the UK, where information sharing across regional forces has become the norm.

Lessons from the UK's Police National Database

The origins of the UK's Police National Database stem from the aftermath of the murder of two 10 year olds, Holly Wells and Jessica Chapman. The case led to the recommendation that local police forces needed to share information.

The man who was eventually convicted of the murders had been in trouble with different local police forces, but moved regularly so a complete picture was never put together. Had it been available, he would almost certainly have been identified as a risk to children and would not have been able to secure a job in the girls' school as a caretaker.

The Police National Database became fully operational in 2011, sharing records on criminals and their activities in a central database. It joins together information from over 43 separate police forces plus a number of other UK law enforcement agencies. The aim is that no matter where criminals have lived in the past, information on their previous activities can be found quickly and easily.

Now, police no longer have to waste time and resources requesting information from each other. More importantly, they can run wider checks on suspects to discover vital information to stop crimes such as terrorism and child abuse before they happen.

Technology supports multi-agency working by:

- Allowing front line workers to view relevant case data from multiple-agency systems at the time of need
- Using current data so police can make informed decisions about protecting vulnerable individuals or the likelihood of further crime
- Setting up security checkpoints so that only those with clearance can view the data
- Creating linked databases that can be indexed and referenced by the relevant agencies as needed.

Taking it mobile

Despite the advances in mobile working, not all forces are currently making the most of its opportunities.

If police officers were able to connect to a central computer via a personal mobile device, it could shorten the chain of communication. Officers would not need to spend time calling into the police office for briefings. Using their secure mobile devices, they would be able to take the briefing information out with them on the street.

Likewise, taking complete witness statements on a mobile device is still far from standard practice and officers are completing the process back in the office.

ACCESSING INFORMATION ON THE MOVE

The option for police officers to access the information they need remotely saves valuable time. It also reduces the need for personnel searching for information at a central control center and relaying it back to the officer.

Accessing this information on the move means that an officer could see right away that the suspicious person they are about to stop is known to five police forces for violent conduct and weapons offenses.

This technology is available now and it is fully scalable, with the option to start small and add more applications and refine the system over time.

Lessons from Helsinki's Rescue Department

Mobile working is being used effectively in Finland by the Helsinki City Rescue Department. Through an automatic vehicle locating (AVL) system, the control center and rescue crews in the field can share real-time information.

With this information, the department is able to ensure that the right rescue teams get to the right incidents as quickly as possible. It also allows crews to be better prepared for incidents by providing up-to-date information on the risks of buildings, such as the presence of hazardous chemicals.

Detailed map views enable the control center to guide, inform and assist the crews at the scene. Crews also have immediate access to details such as the availability of hydrants, or the presence of other utilities which can assist in the emergency.

As a result, the Helsinki City Rescue Department can ensure their crews are precisely prepared for specific incidents, and equipment is used more quickly and efficiently.

Mobile technology allows police forces to:

- Keep more police officers out on the streets fighting crime
- Realize savings in reducing expensive office space
- Speed up administrative processes to save time and money.

Citizen-led policing

Citizens are recognizing that they have a degree of responsibility for their safety and are becoming more active in protecting their own communities. The number of people who mobilize themselves when a child goes missing demonstrates how willing many are to help.

In addition, citizens are increasingly prepared to organize themselves in Neighborhood Watch teams or WhatsApp groups. While the police are exploring the best way of working with these initiatives, there is no doubt that organized citizen groups have a major impact on policing. This growing motivation among citizens to preserve public safety can be harnessed by the police to solve crime more quickly and even prevent it.

Lessons from the Netherlands' Burgernet

Since 2010, the Dutch police have alerted volunteers to help them solve crimes using a GIS application, SMS or telephone alert, in a system called Burgernet ("burger" means "citizen"). On receiving a report of a burglary or a missing child, the police control room operator can start a Burgernet alert.

Burgernet participants receive a voice or a text message giving them a clear description of a specific person or vehicle and asking them to keep a look out. If a participating citizen sees the person or vehicle concerned, they call the free Burgernet number and are automatically put through to the control room. The operator then updates the police with the information. At the end of the Burgernet incident, all those taking part receive a message informing them of the result.

Thanks to the efforts of Burgernet participants, numerous suspects have been caught, missing people have been traced and the police have received useful information. The system has been a huge success. More than 1,000 calls to action are issued each month, 10 percent of which have led to criminals being caught red-handed and 20 percent have led indirectly to apprehensions.

INCREASING CITIZEN ENGAGEMENT

Increasing citizen engagement helps to build and maintain trust within the community. Citizens become known and identified partners who effectively are "social sensors" for the police.

Another Dutch initiative is ComProNet—the Community Protection Network—a scheme to reduce crime associated with local incidents, which is also being trialed in Belgium. The aim of ComProNet is to connect citizens, police, businesses, fire and healthcare professionals at the same location in a single security network so they can use each other's eyes, ears and expertise.

Through a smart phone app, bar and restaurant owners and managers can alert police if incidents have arisen—or are likely to arise—in an area. These reports are automatically redirected to police officers who are closest to the location so that they can quickly reach the spot and prevent the incident.

Citizen involvement can go a step further too. If there is an accident, nearby members of the public with a first aid certification can be alerted via the app and be quickly on hand to provide assistance. Calling upon the skills of willing and responsible citizens opens another avenue of support when resources are stretched.

Technology allows police forces to engage citizens by:

- Gathering information from citizens on crimes electronically
- Analyzing data automatically for trends
- Involving citizens in real time to help capture criminals
- Enabling citizens to self-serve by reporting crimes electronically.

CGI

An invisible crime?

A 17 year-old girl buys tickets online for a music festival only to discover that she has used a bogus website. She has lost €300. The offending site originated in a separate jurisdiction and there is little that can be done, yet she is still a victim of crime.

If someone had broken into her house and stolen €300 from her purse, the police would be able to see the scene of the crime, collect fingerprints and try to catch the thief.

Fighting cybercrime

Cybercrime is an emerging and fast-growing area of focus for law enforcement, prompted by the ubiquitous Internet, which has grown from 16 million users in 1995 to 1.7 billion users today. By 2015, the world will have more interconnected devices than people.[1]

We now live in two distinct communities—the physical and the virtual—where different rules seem to apply. In the virtual world, it is all too easy for criminals to propagate money-making scams, and for cyber bullies under their cloak of anonymity to attack people in ways which are as damaging as a physical assault. Digital channels are a low-risk, high-reward outlet for crime, especially since much of it goes unreported. An estimated 378 million consumers are victims of cybercrime each year and the total global cost of cybercrime in 2013 was US$113 billion.[2]

As a result, on-the-ground police work can no longer be the sole focus of law enforcement. While traditional crimes are an ongoing concern, cybercrime will continue to create new challenges for the next generation's police force.

Many police are understandably struggling to cope with cybercrime, let alone define it. Isolated incidents are difficult to detect and solve, and bringing criminals to justice can be problematic as many of them are located in countries far away. Additionally, continued rapid technology growth presents ever-increasing opportunities for cybercrime.

FOCUSING ON PREVENTION

In some countries, for example the Netherlands and UK, separate units of cyber police have been formed to focus solely on detecting and preventing cybercrime. This is recognition of the fact that policing the virtual community calls for a different approach.

To be successful, cyber police initiatives must work effectively with online sites and Internet providers to enable people to identify and report cybercrime more effectively.

Prevention is one of the most effective weapons against cybercrime. By warning citizens of the latest fraudulent practices being deployed, they can take steps to protect themselves.

Data must play an increasingly pivotal role in identifying cybercrime. For example, police can use predictive analytics to identify suspicious activity to warn citizens not to use certain sites or close sites down before too many people fall victim. Implementing regular and frequent automated analysis of big data can help police identify unusual behavior patterns and close down fraudulent sites more quickly

Technology allows police forces to tackle cybercrime by:

- Identifying patterns that highlight potential fraudulent activity
- Tracking cybercrime across jurisdictions
- Informing citizens of sites or new schemes to avoid
- Working with other agencies to educate young people about cyber bullying.

.

[1] 2010 UK National Security Strategy, "A Strong Britain in an Age of Uncertainty."

[2] 2013 Norton Report, one of the world's largest consumer cybercrime studies, based on self-reported experiences of more than 13,000 adults across 24 countries.

Conclusion

The traditional policing model is no longer appropriate for our changing society. A new approach is the logical next step in the continuous improvement of policing to meet society's needs. The same rapid technology growth that is creating new policing challenges is also creating new opportunities for forces to do more with less and respond more effectively.

Efforts to move toward the next generation of policing can benefit from reviewing the existing best practices and innovative techniques being deployed today that are discussed in this paper, such as:

- Intelligence-led policing
- Shared data models that support multi-agency collaboration
- New channels that increase citizen involvement
- Mobile solutions that promote efficiencies in resource deployment
- Predictive analytics that help combat cybercrime.

Technology can go a long way toward enabling the right resources to be deployed at the right times and in the right places for a more focused approach to both conventional and online crime.

We are seeing a step change in the way agencies, citizens and the police are working together, and the right technology will continue to drive this information exchange forward.

With the prior knowledge that there are children upstairs in a house where domestic violence is taking place, or a tip-off that a group of rowdy sports fans are looking for trouble, policing can be more informed and proactive. This way, the police can save time, money, heartache and even lives by intervening before, rather than after, the crime has been committed.

A fresh look at working practices will open up many innovative opportunities for the police to work together with other agencies, organizations and citizens to create a fundamentally safer society for us all.

We welcome the opportunity to help your organization evolve to support the changing society. For more information, visit www.cgi.com/publicsafety or email us at government@cgi.com.

Why CGI

CGI has built a deep understanding of law enforcement and public protection in Europe, Australia and North America based on close relationships with our clients in this sector Law enforcement agencies partner with CGI because we understand the challenges they face and have extensive experience in integrating systems across agencies. Our innovative solutions help these clients adopt modern and efficient work practices and transform their operations to increase citizen engagement and ultimately create a safer society.

ABOUT CGI

Founded in 1976, CGI is a global IT and business process services provider delivering high-quality business consulting, systems integration and managed services. With 68,000 professionals in 40 countries, CGI has an industry-leading track record of delivering 95 percent of projects on-time and on-budget, aligning our teams with clients' business strategies to achieve top-to-bottom line results.

cgi.com