masonadvisory

WHITE PAPER

FIT FOR THE FUTURE?

The future of IT in police forces

www.masonadvisory.com

Contents

Foreword

The challenges facing police forces in the UK today are more complex than ever. In the face of budgetary pressure and increasingly sophisticated crime, we believe police forces must put IT at the heart of their organisations if they are to succeed in improving crime-fighting capabilities while becoming more efficient and cost effective.

I'm delighted that our research includes the views of several of our clients and partners, each lending their experience, opinions and advice to paint a picture of what the future has in store for IT in policing. Our research highlights seven key areas that fall broadly into two categories: technology and people.

On the technology side, it's clear that the future is mobile, platform-based and interoperable. We explore in detail the impact of mobile and digital technology, the growing importance of data management, what IT collaboration between forces looks like, and options for externally sourcing IT infrastructure.

Of course, technology needs people with the right skills to use it effectively. This report also explores what forces can do to attract high-calibre IT professionals to work for them, how to foster a culture of partnership between IT and the wider police service, and how to overcome the many challenges around governance.

I hope you enjoy the read.

Steve Watmough,
CEO, Mason Advisory

FIT FOR THE FUTURE?
The future of IT in police forces

1 A look into the future

The officer's smartphone buzzes – there's a crime scene to respond to, and quickly. The officer is only three streets away; there is usually a patrol car in the area precisely because it's known to be a hot spot for crime at this time of day. By the time the officer arrives, they've read a briefing on their phone: the key points of the emergency call and the victim's name, address, and history with the police. The officer is also informed of the victim's mental state and is able to greet them with the right level of sensitivity.

The officer records the witness statement with a body-worn device, then takes photos of key evidence and scans fingerprints using a tablet, all of which are immediately uploaded to a national database hosted securely in the cloud. While the officer talks to the victim about what will happen next, an algorithm runs in the background to identify traits of this crime that are similar to others recorded in the area, while checking fingerprints and other evidence to see if there are any matches. The algorithm uses analytics to determine if this bears the hallmarks of a random attack, a crime of passion, or part of a pattern of ongoing abuse. Within minutes, a briefing arrives in the inboxes of an investigative team back at the station, with the details of the crime, a list of suspects, their location, and any other relevant information the police database holds. The investigation begins immediately.

Having reassured the victim, the officer receives a briefing about the next crime on their device and heads straight there. By the time the officer returns to the station that evening, a suspect has already been apprehended.

2 Universal barriers, converging needs

This scenario may seem a long way off to many working in policing today. The police service has been under extreme pressure to reduce costs and is already into a third round of rationalisation. Forces are being asked to do more with less while at the same time being asked to build new capabilities to fight modern crime. It feels like an uphill slope that keeps getting steeper.

For IT departments, the slope is particularly steep. The natural reaction of police forces is to protect the frontline officers, knowing that cuts here are never popular with the public. Often, police forces are asked by journalists about their ratio of frontline staff to support staff, with the implicit suggestion that savings should be made in the back office before touching anything operational. From this perspective, support functions are the easiest place to start looking for cutbacks.

Increasingly, forces are relying on technology as the answer to doing more with less – a means of simultaneously saving money and improving crime-fighting capability. Many forces are already making headway in shared services, outsourcing and collaboration, but in a world where technology evolves at a runaway pace, it's hard for forces to keep up. As seasoned IT professionals in policing will know, upgrading systems and reshaping operating models around them is hardly a straightforward task, and there are some universal barriers that all forces face.

Matters are made more difficult by the incredibly complex IT landscape that has mushroomed across the country following the decision to hand responsibility for IT decisions to each individual force. Decision-making at a local level means forces can press on with their own procurements but does not encourage the standardisation required to help forces collaborate easily. An outsider might ask why the government doesn't just centralise IT, imposing top-down solutions for all forces, but this approach has failed twice in the past.

To top it all, police operate in a very risk-averse environment – after all, it's a vital public service, upon which we all depend to keep our neighbourhoods safe. The availability, reliability, and performance of IT systems are critical to ensuring officers can do their jobs. Yet as with every other area of policing, IT departments are expected to meet these demands and implement change with smaller budgets and fewer resources. It mustn't be underestimated how hard change is, and the capacity for mistakes means that some would rather not attempt it. No force wants to be on the front page of the *Daily Mail* explaining how it lost confidential information, and this fear can have a paralysing effect.

Yet despite all this, there is evidence that these shared challenges mean the needs of different police forces are aligning, and there is optimism that technology offers a way to ease the pressure police forces are under. From talking to senior IT resources and industry experts, as we as drawing on our own experience of working with the police, Mason Advisory has distilled these conversations into seven areas of focus for police forces in the UK today:

- mobile and digital technology (moving away from paper-based systems)
- more effective data management
- collaboration
- giving IT departments a more strategic focus
- attracting the right skills for those departments
- engaging with the wider force
- and, making sure governance arrangements encourage real transformation.

3 Contributors

- Scott Phillips, *Chief Technology Officer*, **British Transport Police**
- Nick Alston, *Police and Crime Commissioner*, **Essex Police**
- Ben Rowntree, *Chief Information Officer*, **Surrey and Sussex Police**
- Richard Thwaite, *former Chief Information Officer*, **Metropolitan Police**
- Jules Donald, *Head of ICT*, **Kent and Essex Police**
- Mark Hanby, *Director*, **EY**
- Tony Dawson, *Deputy Director*, **Methods Advisory**
- Harj Singh, *Principal Consultant*, **Aristi**
- David Cohen, *Principal Consultant*, **Mason Advisory**
- Jon De'Ath, *Principal Consultant*, **Mason Advisory**
- Rob Watkins, *Associate Director*, **Mason Advisory**

4 The future is mobile and digital

When considering the many demands placed on police officers, it's widely agreed that filling in paperwork is not the best use of their valuable time. "We've got to get rid of pencil and paper, and stop officers having to go back to the station and type things up," one senior IT resource tells us. Mobile and digital technology offers the opportunity to save time and money, while also providing an improved public service.

It's already having an impact, reducing the hours officers spend on time-consuming reports and enabling them to be more visible to the public. "They can get out there and receive location-based briefings delivered in a mobile, agile way," says one interviewee. The functionality available on modern devices allows officers to take witness statements, take photos and footage of evidence, and even access criminal intelligence on the go through secure apps, removing the need to get back to the station to search databases or file evidence.

With better information and less time spent on paperwork, it's no surprise that mobile and

digital technology is popular with officers. "Cops are increasingly tech savvy," says one person we spoke to. "Often they're disappointed they can't use the technology they have at home at work. Cops love a bit of new kit, and they want to be able to use it in the workplace." It's IT change that the rest of the organisation can feel excited about, and it reassures both officers and the public that the police are adequately equipped with the devices they need to fight modern-day crime.

Indeed, public confidence has many reasons to increase with the roll-out of mobile and digital technology. "They're seen to be using the technology that everyone else is using – they don't get the little black notebook out anymore because they have tablets or mobiles," says one interviewee. The public's expectations around the way they interact with the police are changing, including the availability of digital channels. In the same way that banking, retail, and many other industries have evolved their customer service, the police will increasingly be expected to do so as well.

"The public are questioning why they have to go in person to a police station to report a crime, rather than report it online," says one industry expert. By enabling digital services, the public will be able reduce the number of face-to-face interactions by dealing with minor queries through cheaper online channels.

There's also an economic case in favour of decommissioning ailing legacy systems – which are expensive to maintain and require specific in-house resources to run them – and replacing them with mobile and digital technology.

This may not be popular with existing back-office staff, but is vital to realising the financial benefits and reducing the complexity of the IT architecture by upgrading to modern applications.

4.1 New technology, new problems

Naturally, new technology will create new problems. One pressing issue will be trying to process and understand the vast amounts of data that forces will be able to capture. "Digital evidence and digital asset management is a major challenge for us – an area we are actively progressing in terms of programmes and projects," one senior IT resource tells us. "There are massive amounts of data – from phones, CCTV, computers. It's a huge increase." While certainly a challenge, it's also a major opportunity for police to up their capability. Information that is shared via email today will soon be shared through digital interfaces, linking officers to case workers and to the courts and justice system. As that volume of information increases, digital interfaces enable each party to access and process the information they need directly, cutting the time a case takes to move through the system.

It's widely agreed that filling in paperwork is not the best use of officers' valuable time.

Of course, getting rid of the old and ringing in the new is easier said than done, and while the benefits could be transformative, many forces have a long way to go. After years of underinvesting in IT, the hurdles can seem impossibly high. "We don't really invest in our technology and stay ahead of the curve, and we don't change much because it's so difficult," says one senior person we spoke to. "We need to be fully operational all the time; we can't have down time."

This pressure has led many forces to be reluctant to decommission legacy systems and applications in favour of newer technologies, preferring to build hybrid solutions on top to meet whatever the new requirement is. It's seen as a lower risk option, but it contributes to the complicated architecture, and discourages police services from implementing transformative IT change.

4.2 What can forces do to be successful with digital and mobile technology?

Learn from previous experience. Despite these barriers, the police service has form when it comes to mobile technology. Having implemented mobile technologies in the past, there will be plenty of people already working for the police with vast experience to draw on. "Forces need to learn the lessons from previous mobility projects to assess business benefits and lessons for what can be improved," says Rob Watkins from Mason Advisory. "They should think about what will provide the best efficiency in terms of resource and process. It shouldn't be technology for technology's sake."

Refresh, don't replicate. It's important that IT doesn't try to replicate the paper process with digital technology. Instead, implementing new systems should be seen as an opportunity to renew and simplify processes and to manage data more effectively. One senior IT resource describes how they are reviewing all their applications and procuring a new platform that brings together all the functionality the force needs. By rationalising applications and creating one point of information, they'll not only save time and money, but also create a data warehouse providing a single, accurate version of the truth.

It's easy for forces to slip into thinking tactically about te chnology rather than strategically.

Think strategically, not tactically. It's easy for forces to slip into thinking tactically about technology, especially when under pressure to deliver solutions with less money and fewer resources. Another temptation when central funding is available for specific projects is to create an incentive to deliver a point solution by a certain date, rather than thinking about the organisation as a whole. Both tendencies must be resisted in the interest of taking a holistic, strategic approach.

4.3 Enabling mobility through the Emergency Services Network

Police forces are preparing to replace Airwave with a new mobile communications system, the Emergency Services Network (ESN). Airwave was leading technology when it was deployed, but it's not able to provide the broadband data services that users increasingly need. The procurement of new technology for the ESN aims to enhance the services available to users, but also to increase the flexibility and affordability of these services.

Every police force in the country is collaborating with the other emergency services and government departments in a programme that will include around 230 control rooms, 50 000 vehicles and about 300 000 devices. It's a huge task, spread over some four years once contracts are awarded (scheduled for the summer of 2015). ESN is intended to replace the critical voice functionality currently provided by Airwave, as well as providing access to high-availability mobile broadband with extended coverage that could be used to support future mobile applications on a range of user devices.

While this presents clear opportunities for extending the use of mobile apps, forces must also consider the organisational impact of such a change. Replacing all the current devices and associated control room systems with the new ESN and associated 'smart' devices will have a major impact on every force in terms of supporting the technology change, integration with control room systems, adapting working practices and training users.

Another challenge is that all forces have to consider how their control room systems and operational practices will integrate with the ESN from 2017, but because the ESN specification is loosely defined, it's proving an immensely complex process.

Lessons are, however, already being learned: "The ESN procurement has demonstrated a way of bringing stakeholders together in terms of gathering requirements," one senior IT resource says. "This time the engagement has been better – it's not just been one set of requirements imposed on everyone else, but a more collaborative approach."

5 Harness the power of data

"I'm sure all police forces have valuable data sitting in different databases, but if we had the opportunity to put it into a single entity it would be very powerful," says one senior IT resource.

Indeed, the benefits of having reliable data and using it intelligently can already be seen in the rise of evidence-based policing. Technology is able to look at crime statistics for an area and target patrols at set times, resulting in a major reduction in crime in areas where this tactic has been used. Technology can also help with the analysis of data to assess how successful this approach has been and where it might need flexing to be more effective.

Looking beyond data held by the police, the ability to analyse data from local authorities, the probation service, the NHS and emergency services would no doubt strengthen the police service's ability to respond to and prevent incidents. In the longer term, understanding what data you have and where it is will open the door to big data and analytics, and even the realms of predicting patterns of behaviour.

Just as relevant, though it may not sound quite as exciting, is the fact that having a handle on available data can simplify many other things that IT departments need to do. Externally sourcing aspects of IT infrastructure and collaboration with other forces are two of the key areas forces need to act on to reduce costs, and both efforts can be aided by a tight data management regime that understands exactly which data falls into which security classification, where it can be stored, and who should have access to it.

5.1 What's preventing forces using data more effectively?

Forces are, however, a long way from this level of data management and analysis. Most don't have a clear understanding of what data they have, and therefore don't have adequate governance around it. "There are lots of old and diverse systems," one person told us. "We try the best we can, but there are silos of data. We don't always have the mechanisms to get the data, and there are worries about reliability." Reconciling and cleansing data can be a long and expensive process, and it may well put many forces off proactively doing it.

5.2 How can forces get a handle on data?

Shift the focus from system ownership to data ownership. Similar data may be in different databases, so it needs someone looking at it from a data perspective, rather than a system perspective, in order to link it up and give it meaning.

Own your data – wherever it is. Whether it's in house or managed externally, IT departments need to take ownership of police data. It could be easy to outsource and forget, but it's the police that will be on the hook if something goes wrong. It's down to the force to take ownership of the integrity, quality, security and access to its data.

Implement an information assurance regime. Some forces are already doing this, others need improvement, but it's absolutely essential to establish the governance around who owns which data and what security classification it needs. Information assurance experts should be engaged early on in any project, and checks must be put in place at project gates to ensure the organisation is adequately engaged. If the project hasn't engaged with the rest of the force to understand the information security requirements, the project shouldn't pass that gate. Forces should aim to follow the

CONTRIBUTOR VIEW

"I worked on a body-worn video project, where the technology enabled officers to capture videos and download them to a central repository. What the IT department hadn't done was check the security requirements when downloading. It didn't comply, and it meant anyone on the network could see it. The IT department hadn't asked the security team about their requirements – they just wanted to get it done as quickly and cheaply as possible."

government standards developed by Communications-Electronics Security Group (CESG), which may sometimes get overlooked in the rush to pilot new solutions.

Seize the day. Some forces are tackling their data at the same time as other major IT change in their organisation – after all, it makes sense to fix everything while the bonnet is up.

Such big, systemic changes are not necessarily easy to plan. As a result, they may not happen until forced by outside events, as one of our interviewees candidly explains: "Changing our systems has been a great opportunity to cleanse and reconcile our data, but that's because the contract for that system happens to have ended – it's by luck rather than design."

6 Prepare to collaborate

Do criminals respect the boundaries of police forces? No. Do they use technology to collaborate within the UK and internationally? Of course they do. Do the police? In some cases yes, but in too many others the answer is no. To fight modern crime, the police need to work together to build their IT crime-fighting capabilities. And in the context of budget cuts, the only way to do this is through greater collaboration.

The pressure to join up in terms of sharing information, working across geographical boundaries, and combatting the changing profile of crime means some forces are already beginning to work together. The Athena project, involving seven forces, is an example of police forces collaborating to reduce costs, cut bureaucracy and increase capabilities. "Athena will be a massive step forward," one senior IT resource tells us. "To put it in perspective, we had separate systems for everything – child protection, custody, case preparation, and so on – Athena means there'll be one database, and we'll be sharing all that information with seven forces."

In addition to operational systems, back-office functions are also a major opportunity to reduce cost through collaboration. Providing a regional IT service creates the opportunity to reduce the hundreds of systems and applications used across multiple forces to one single point of information. The reduction in maintenance costs, the removal of duplication, and the simplification of the technical landscape would save the police service millions each year.

Of course, programmes to merge capabilities are expensive and hard to do, but it may be that the police service's hand is forced. Several people we spoke to during the course of this research mentioned the likelihood that further collaboration will be legislated at some point by the government. Indeed, Sir Bernard Hogan Howe, the head of the Metropolitan Police Service, called for the creation of "no more than nine" regional forces in December 2014, with a view to creating common infrastructure and upping police capability to fight the crime of the future.[1] Forces in England and Wales need only to look north of the border to Scotland's successful merger of eight forces into one, saving GBP72 million in the first year alone.[2] "The Scottish police force is the template for it, and that was legislated in," says one interviewee. "It'll go much the same way here."

6.1 Barriers to collaboration

Until then, there are several factors standing in the way of building collaboration and shared services. Perhaps the greatest complication – and the one from which most others stem – is that the current set-up does nothing to encourage forces to work together. "Although we know a lot of money could be saved by rationalising the number of systems being used across the UK's forces, there's no compulsion on people to move," one senior IT resource says. In the majority of cases, there is no national direction or recommendation around

[1] http://www.theguardian.com/commentisfree/2014/dec/14/reform-cuts-public-risk-police-emergency-services-austerity
[2] http://www.bbc.co.uk/news/uk-scotland-26690304

how best to collaborate. And so, rather than begin down the fraught path of attempting to negotiate agreements among themselves, many forces simply press ahead with their own solutions to meet their immediate needs.

This habit might not be so bad if it weren't for the fact that many forces are reluctant to fully phase out legacy systems, contributing to incredibly complex IT architectures which are unique to each force. And even when forces do collaborate, they often keep their legacy systems going: "Many police forces still have opportunities to rationalise IT infrastructure and services at a local and collaborative level," says Rob Watkins from Mason Advisory. "They're still supporting individual systems, then building hybrids to collaborate with other forces, but maintaining the original individual system." One person we spoke to said simply that building on top of existing systems is "just how we work". The police are used to finding quick fixes for IT issues, rather than taking a strategic, long-term view about their transformational needs. Ultimately, forces will not realise the benefits of new technology so long as they stay invested in the old world.

"The Scottish police force is the template for it, and that was legislated in," says one interviewee.

Habit aside, one of the biggest reasons forces are reluctant to overhaul ageing systems is, of course, pressure on police budgets. Shared services and systems will allow police forces to rationalise, but may require big up-front investment – money that forces may not be able to find or may not get the stakeholder support to spend. There can be push back on making the investment needed, so rather than scrapping a system that's no longer fit for purpose, forces find a sticking-plaster solution to solve the problem. It's more acceptable to ask for GBP100 000 to fix a problem in the short term, than to secure a GBP2 million investment to scrap an ailing system entirely and get the system they really need.

Funding is further complicated by Home Office policy, which doesn't always lend itself to collaboration. "One of our biggest challenges is the Home Office innovation funding – we are top-sliced and have to bid for bits of technology, and it doesn't promote standardisation," one senior IT resource says. "An example is body-worn video – it ended up with eight different procurements across different forces, rather than one central process."

Another cause of difficulty is the position of national systems in this landscape. Police forces are already struggling to finance the improvement of their own systems, yet the government is asking Police and Crime Commissioners (PCCs) to take control of yet more national policing systems. "Every one we've looked at so far has been in a pretty ropey state," says one senior police resource.

The autonomy that forces have become used to exercising has led to 43 different ways of doing things, breeding behaviours that make change harder. For all the talk of collaboration, human nature can get in the way: forces accustomed to acting autonomously often say they're happy to collaborate, when what they mean is they're happy to collaborate as long as it's their solution that is adopted. "Even where formal collaboration is in place, the different forces still tend to do their own thing," says David Cohen from Mason Advisory. Indeed, the personalities leading policing are necessarily strong, but the political environment can make it very hard to develop a collaborative culture. "My force is looking at collaboration, but personality and politics is a huge barrier," says one interviewee, "To get two chief constables working together is pretty good – any more than that is a near miracle."

6.2 What steps should forces take to ease collaboration?

Develop an IT strategy. After years of hierarchical development without a strategy, many forces will benefit from benchmarking

CONTRIBUTOR VIEW

"I still find it hard to understand why you need 5 or 6 different intelligence systems to choose from that basically do the same thing, yet forces have been allowed to procure different ones."

and baselining their current infrastructure to understand the strengths, weaknesses, and priority areas to be addressed.

Keep collaboration in mind when choosing systems. Ensure IT systems that are deployed are based around a well designed architecture and on open standards that make it easy for different systems – and forces – to interoperate. Forces should move away from inflexible monolithic systems, instead choosing systems that enable them to be responsive in the future. "CTOs and CIOs are aware that their business is likely to have to change in the next five to ten years," one industry expert says, "So they recognise the need to buy technology that enables the organisation, rather than be a blocker to future change."

Be willing to decommission legacy systems. And to do that, ensure the change management is in place to drive different behaviours and aid the transition to the new way of doing things. It's the only way to simplify the IT landscape and to realise cost savings.

Use industry-standard technology. It's reliable and interoperable. Some forces have made the mistake of rushing into cutting-edge technology, but exciting as it can be, it can cause issues further down the line if it's untested.

Lobby for a national strategy. Some of our interviewees lamented the lack of central guidance. Although a top-down approach has failed in the past, a less draconian approach that offers guidance without dictating the exact pieces of technology that must be used would be welcomed by many. "I think we need a much clearer landscape on enterprise architecture, and every force using that national strategy," says one senior IT resource.

6.3 Collaboration tool of the future? The Public Services Network

The implementation of the Public Services Network (PSN), the government's programme to unify the provision of network infrastructure across the public sector, illustrates how collaboration could work and some of the issues it throws up. For forces, it's replacing the Police National Network (PNN) and requires them to ensure that their IT policies, security, governance arrangements, and systems are compliant by October 2015.

The PSN has the potential to enable greater collaboration and cost reductions through the sharing of services and new opportunities, such as outsource models, external cloud and secure hosting of services. It'll also enable a secure means for sharing information with local government, the health sector, and the emergency services that are also on the PSN. "Combining these into a single solution, sharing data more effectively with the prison service, probation, and other government agencies – it's absolutely vital to the future of policing," one senior IT resource says. As well as enabling collaboration, the PSN should de-risk procurement, as all providers will have to meet government standards. "The PSN is like the Apple App Store – you know that apps are developed securely there, so are happy to buy them," one industry expert says. "The PSN means forces can buy services with confidence, and it saves procurement costs."

Despite this, not everyone is convinced of the upside. "In terms of benefits, the jury is still out," one person tells us. Another says: "It's up to you how much you benefit from the PSN. It doesn't have to mean huge change – if you use PNN and use the PSN in the same way, then it's easy."

Ultimately, the perception of the PSN's usefulness may depend on how easy or difficult it is for each particular force to comply, and some forces already feel swamped by compliance requirements. "It's a nightmare – we have fewer people than we should have to deal with it," says one interviewee. "Each time we have compliance requirements to meet, it paralyses us for a few months." The new compliance requirements have certainly driven vast amounts of work, and called time on some of the older parts of the police's IT infrastructure, which simply can't be made compliant. "The police have to rationalise and transform many old legacy IT systems, and it's opening opportunities to review data centre

strategies and external hosting services," says Rob Watkins from Mason Advisory.

What can police forces do to ease the transition? Forces need to proactively assess if they are ready for the security compliance requirements and make sure they understand the data that they manage. That means having a clear view on the different levels of data sensitivity and whether their data is being handled appropriately. Forces also need to think beyond simply complying: "Most of the effort is consumed by organisations designing technology to comply with standards for the PSN, and not enough thinking goes into what they're going to do with it once they are compliant," one industry expert says.

Perhaps the most important thing IT departments can do is change the narrative to view PSN compliance as a positive step – an opportunity to take a health check on their procedures, systems and data management, rather than as a mere box to tick.

7 Externally source what can be bought, develop internal capabilities for what can't be

Police forces don't have the budget to increase crime-fighting capability while simultaneously maintaining their entire IT infrastructure in house, so alternative models must be considered. One significant opportunity is the outsourcing of services that can be bought as commodities, freeing internal staff to assume more strategic roles. "Our operating model will have to be aligned to outsourcing some of the areas you can buy as commodities and SaaS in the future," says one senior IT resource. "We need to buy those services, rather than maintain them in house."

Remote cloud storage and outsourced data centres stand out as particularly promising candidates for external management as the amount of data police forces need to handle, store, and analyse keeps growing. "Data storage is a massive issue," says one interviewee. "There's terabytes and terabytes of data from digital evidence, body-worn video, CCTV… Internal data warehouses won't be feasible, so we're looking at cloud storage."

The size of the challenge has prompted a change of attitude towards remote storage, and some forces are already reaping the benefits: "The good thing about our data centre is it's a platform as a service – we rent stuff rather than buy it every four or five years," says one person we spoke to. "It's about a third of the cost of buying the stuff, and we don't have to do the refreshing and maintaining ourselves." Some may have reservations about data security and the security credentials of providers, but the introduction of the PSN should mean procurement fears are alleviated. And the potential cost saving should prove an adequate incentive to get a handle on security clearance required for different types of data: "As long as you know what security clearance you need, you can absolutely use the cloud," one senior IT resource says.

Other areas to consider are the 'run of the mill' elements – desktops, office applications, and so on – which can be outsourced quite easily. The PSN may even enable some secure systems to be outsourced, where there are appropriate external providers available. Areas of customer interaction, such as first and second-line support could also be considered if companies can offer a managed service (avoiding the pitfalls that the NHS's 111 hotline ran into), and the hands-on implementation of much of IT can be done by external, temporary resources.

7.1 A more strategic focus

Moving to a consumption-based model changes the skills needed in house, enabling the creation of a smaller, but more strategic IT function. "What we need is an intelligent internal client function," says one interviewee.

CONTRIBUTOR VIEW

"The skills we have in IT at the moment reflect that we just try to keep applications and systems running – it's the legacy of IT."

This function needs to be focused on strategy, planning, solution architecture, risk, partnering with other police functions, and commercial and supplier management to ensure outsourced providers are procured and managed effectively. Engagement with service providers is particularly important from a risk perspective. "The police service can never outsource the risk," one industry expert says, "so it's vital that risk is managed internally, and that forces are sure they are complying with the security standards they need."

7.2 What should forces consider when thinking about outsourcing?

Assess the activities taking place in house today versus what that could look like in the future. Look at the types of activity IT organisations typically undertake and gain an insight into which ones are transactional, commodity skills. For example, technically delivering standard repeatable activities are skills that could be bought.

Drive internal staff up the value chain. Internal roles should focus on the areas that can't be outsourced or are better retained in house, such as programme management, strategy, supplier management, planning, and system architecture. Strategically focused roles will ensure that systems being built are compatible with what forces will need in the future and may also help police departments in attracting high-quality talent that might otherwise prefer a career in the private sector.

Adopt a risk-based approach. Look realistically at risk and establish the levels of risk that are acceptable within the organisation. Each force will have a different risk appetite to be catered for; adopting an intelligent risk-based approach will cut down on over-cautious and unnecessary spend.

8 The importance of attracting the right people

In repositioning IT to be a strategic function and business partner with the rest of the organisation, it's crucial that the department attracts the calibre of people with the right skills to gain credibility with the rest of the police. After all, the police could invest in the most cutting-edge technologies, but if they don't have the right skills to use them effectively, it's all rather pointless. It's an issue that becomes even more pressing as resources shrink. "What will the IT department of the future look like? They are going to be smaller – they can't afford to be the size they are today," says Rob Watkins from Mason Advisory. A significant proportion of the costs of IT departments are human, so it's vital that budgets are spent on the right people.

In their slimmed-down form, IT departments of the future will not only need technical skills but management skills, commercial skills, and analytical skills, too. Attracting high performers, which can already be a challenge, will only become more important: "The people with the analytical skills we need are attracted to the private sector," says one person we spoke to. "Top analysts earn more money there." In addition to pay, top IT professionals are also lured to the private sector by the size, prestige, and cutting-edge technology available in the corporate world; police forces need to seriously consider how they can compete.

While it isn't a problem across the board, some forces do face issues with the IT workforce that they have at present, with one senior IT resource describing the approach as "old fashioned". Another laments that the IT function sometimes accommodates retired officers who may not have the right technical skills for the job. A narrow outlook prevails in some IT departments, with some people unwilling to take on tasks that go even modestly beyond their role description. "Some people are orientated around the old world, where one person looks after one application, and that's their job," says one interviewee. "We need to change their mindset away from that, to be able to do more things than just the one thing they do." A pervasive 'this is how we've always done things' attitude creates the sort of inertia that can make change fall at the first

hurdle: "Having the intelligence and the nous to realise this opportunity in your organisation and to exploit that – that's where we fall over," says one senior IT resource.

8.1 How can forces attract the skills needed for the future?

Create a career path out of change management. Nurturing individuals with the aptitude and tenacity to lead change programmes will be essential to building in-house capability. There needs to be a career path for these skills, and it needs to be as valued as gaining operational experience. The brightest and best need to see a path to the top of the organisation, and that their career can be enhanced by delivering challenging change programmes.

Get IT to the top table. The police service will struggle to attract high-calibre people until IT is integrated as a true business partner with an equal voice when taking decisions about operational policing. Forces can begin by ensuring IT representation at key meetings, and building a culture of partnership between IT and the rest of the organisation.

Shout about the fact that there'll be ground-breaking work to do. Over the coming years, the police service will be delivering ground-breaking work in security, data management, and crime analysis so let people know that forces are planning big things. It'll help attract people who are really interested in pushing back the boundaries of technology.

CONTRIBUTOR VIEW

"Essentially, we need people who understand how to analyse and capture requirements. Police officers may come with good ideas, but they then tend to buy a package from the first sales person they meet. We really need professional people who understand how to pull a business case together, and better procurement processes."

9 Foster a culture of partnership between IT and the business

It's clear that technology is only becoming more integral to how the police operate, so it's vital that IT is not viewed as a separate, back-office function – IT needs to work in partnership with the rest of the organisation. It's essential that operational policing is involved in IT change to ensure the right solutions are found, and that those who will be reliant on the technology have ownership over the requirements. After all, it's the police officers who will be using the new technology day in and day out.

It's fair to say that the relationship between IT and the rest of the police force isn't always what it should be. To a greater or lesser degree across forces, there is a disconnect between IT and the rest of the organisation. In some forces, IT departments have struggled to deliver on business cases in the past, breeding cynicism about whether technology can deliver the benefits it promises. In other cases, the lack of a coherent IT strategy has led to a 'shopping list' approach, in which the organisation expects IT to comply with a long list of requests without any strategic assessment, contributing to a more complex architecture in which any semblance of strategy becomes obscured by the sheer number of applications. It's a vicious circle. Without a clear IT strategy, departments end up taking the easy route of bolting on a new application or system to meet each new need. And the more systems are piled on, the more complicated the landscape, and the harder it becomes to take that crucial step back to develop a coherent IT strategy.

Furthermore, the police style of 'command and control' makes it harder for IT departments to push back on requests to 'just get it done', even when a more considered approach might be better in the long run. While an unshakeable chain of command is no doubt vital to operational policing, it can be unhelpful to the design, planning, and execution of IT change. The higher echelons of the police are used to giving an order and having it followed without question. As a result, the IT function is often expected to change course mid-stream, further muddying the water around the strategic purpose of technology and upsetting the course of change programmes already in train.

Because the IT department is viewed as existing to serve other parts of the organisation, it can be undervalued, and that makes it harder for IT

CONTRIBUTOR VIEW

"Anecdotally, I've heard of instances where police officers have been given laptops and tablets, and they just turn them over, put their notebook on the back of it and start writing in that. They were just given technology without the additional business change activities required to derive the benefit from the investment in the technology."

to gain the traction needed to push transformational change. "They tend to carve people out for specific tasks, but to get people focused on totally revamping IT is a challenge," one senior IT resource says. And the fact that IT often works in isolation can mean all sorts of problems: misunderstanding security classifications; missed requirements meaning new technology doesn't work as police officers expect it to; training needs that are underestimated; and new processes and technology that don't successfully embed because officers haven't been trained adequately.

However, there is evidence that attitudes are changing: "The traditional attitude to IT within the police is that as long as IT is quiet and cheap, you can sit in the corner and we'll be nice to you," says one interviewee. "Now that we're moving to mobile policing, technology is now more important, and you get a seat at the top table."

"There's a realisation that the police can't achieve the mission they've been set without a strong and flexible IT capability delivering robust, reliable services and driving innovation at the centre of it," says Jon De'Ath of Mason Advisory. It's important that IT catch this wave, and take it as an opportunity to improve the way IT functions engage with the rest of the organisation.

9.1 How can IT functions change their relationship with the rest of the police?

Ensure there is a business representative on all projects. "Most IT projects, if not all, should have senior police representation to support business change and align operational requirements," says Rob Watkins. It's essential if the right solutions are to be found for officers in their day-to-day jobs. But often there is a perception that the police representatives need to have prior technical knowledge, which can result in a reluctance to get involved. "It shouldn't be too onerous," one industry expert says. "If you focus on defining requirements in terms of outcomes rather than technical terms, it'll help IT and the police work together more effectively, using language everyone understands."

Ensure requirements are holistic. It's important to think about requirements at an organisational level, and how the project affects other areas of the business. Taking an overall view will help position the project within the wider strategic direction of the organisation.

Communicate the IT strategy. There should be a clear IT strategy that is communicated and – most importantly – understood beyond the IT function. Explaining in layman's terms how the IT department needs to change to better serve police officers is vital in building a common understanding of the purpose of IT and managing expectations around what can be achieved.

10 Overcoming the challenges of governance

A critical part of any change programme is ensuring the appropriate governance structures are in place. In the world of the police, this can be particularly challenging for two reasons: first, it takes a very long time to move through current governance processes; and second, by the time a project has moved through the process, the leadership may well have changed, in which case the project might not be so important any more, and the new leadership may want to do something different.

The stakeholder landscape for the police can be particularly volatile. Chief constables are often only in position for two to three years, so direction and priorities change frequently. In addition, the multiple priorities of the PCCs, local authorities, and the Home Office must all be taken into account. This creates a constant feeling of changing stakeholders, uncertainty

over budgets, and a lack of commitment that is counterproductive to long-term transformational change.

It's unsurprising that it can take time to navigate this maze of stakeholders to gain approval, even when there is support for what you're trying to do. "We've got a great degree of buy-in around what we want to do with technology, with strong support from the chief and deputy, but it doesn't half take time to get things done," one senior IT resource says. Combine that with lengthy procurement processes, and the hundreds of different applications with different owners, and it's easy to see how projects and programmes can fall out of kilter with each other.

For all the reasons outlined in this report, transformational change in policing is no easy task, so it's understandable that some chief constables, knowing their tenure is likely to be short, steer clear of embroiling themselves in difficult IT transformation.

So how can forces strengthen governance around transformational change? Lead from the top, deliver from the layer below. Of course, change needs to be championed from the very top of the organisation, but if the leadership is also responsible for driving the change, there's a risk they'll have moved on before the programme is completed. To ensure continuity in the people actively managing change, police could look a layer below the top, where typically the churn rate is lower.

CONTRIBUTOR VIEW

"It's often hard to work out who's responsible for change. It doesn't fit into a specific portfolio and you can't escalate everything to the chief constable. Governance will be a key enabler here."

11 Conclusion

Thinking about how to tackle all the issues facing policing can feel exhausting, especially when each is intertwined with several others. The answers will not be the same for all police forces, nor will the steps to get there be a 'cookie cutter' solution.

But the police service should take comfort that commonality is emerging in the ways police are using IT to transform the way they operate.

To rise to the challenge of combatting modern crime with fewer resources and less money, the future of IT will be platform-based – consolidating fragmented applications – digital, and interoperable. IT departments will move to a consumption-based model, outsourcing the services that don't have to be kept in house. To make the big cost savings, back-office functions will need to collaborate and merge, so IT architecture will need to be built around open standards to smooth that transition.

Ultimately, transforming IT means transforming the entire operating model of police forces – it's about IT-enabled change that goes right to the heart of how the police forces of the future will work. To build an infrastructure fit for the future, IT departments need to work in partnership with the rest of the police, establishing a common set of goals that resonate with everyone from a police officer on the beat, to a PCC, to someone in IT procuring a new application.

With everyone moving in the same direction, the steep slope won't seem such a slog to climb.

Mason Advisory would like to thank all the contributors to this white paper – and particularly our partners and police clients – for their time and thoughtful responses to our questions.

We hope you've enjoyed reading our research, and we'd love to hear your thoughts on the issues affecting modern-day police forces.

If you'd like to talk to us about police IT, then give us a call or email our team using the details provided on the back page of this paper.

12 Case studies

Supporting collaboration in the South East with SEPSNSA

We worked with four police forces to negotiate a landmark deal with BT to provide a secure regional network and services, enabling each force to save money, work together more effectively, and protect frontline services.

Each force had its own complex network contracts for different technologies and services – in common with most forces in the UK – so the potential to collaborate, simplify IT, and save money was vast. Mason Advisory started by reviewing existing voice and data networks and associated technologies for each force to establish a baseline from which the future requirements could be understood.

This work enabled the police services to come to a shared vision, defined objectives, and agreement about where efficiencies could be found. We then worked with the forces to develop a business case, providing strategic, economic, commercial, and management recommendations for a collaborative sourcing strategy.

The next step was to determine the best procurement route. Mason Advisory worked with the forces to define requirements that would challenge the market to innovate. The requirements looked for tenderers to demonstrate capability and innovation through their technology and commercial proposals in a way that was new to policing. It ensured the solution found was innovative, transformational, and could deliver on the business case.

The South East Police Shared Network Services Agreement (SEPSNSA) framework will drive significant savings of up to 20% by standardising technology and service models, enabling economies of scale, and creating cost-effective networks. On the contract award of SEPSNSA, SRO ACC Amanda Cooper, Director of Information, Science and Technology for Thames Valley Police wrote: "The forces involved would like to recognise the contribution and project management that Mason brought to the project in delivering this landmark contract for the policing region."

In her speech in November 2013 to the think tank Policy Exchange, Home Secretary Theresa May recognised the SEPSNSA programme as a landmark contract designed to transform the IT technology used by the police forces, enabling them to save money, share information more effectively, and deliver a better service for the public.

A strategy for leading-edge police IT in a modern metropolis

Hong Kong has a comparatively low crime rate, and the police rely on the latest IT to keep it that way. But technology brings increases in data: body-worn video, social media, biometric profiles to name but a few. Being able to use such information effectively is one of the biggest challenges facing modern police forces. We worked with Hong Kong Police Force (HKPF) to rationalise the numerous systems it had developed over the last 20 years – some of which were outdated – in order to harness the power of the information within them.

This work was undertaken as part of our assignment to develop the force's first integrated IT and communications strategy, providing it with a blueprint for the next six years. The force has 37 000 staff, and our team – based in Hong Kong and the UK – undertook a series of interviews and workshops, as well as processing questionnaires from users, to capture a representative view of current ICT provision. We spoke directly with over 150 staff, as well as engaging with 20 external stakeholders from relevant government departments. Combined with a detailed review of ICT documentation, this in-depth consultation led to the development of an as-is assessment report into the infrastructure, application architecture, service provision and ICT organisation.

We then undertook a gap analysis to assess what the force needed to do to move from its existing position to its desired future state. Specific attention was paid to a number of core technologies including mobile communications, fixed-line telephony, communication with the public, the desktop estate, and all operational applications. A number of particular areas for improvement were identified to enable HKPF to leverage the latest ICT – and the operational improvements it could bring. Our final strategy report (including detailed costs) specified a portfolio of recommended projects and implementation priorities.

Recommendations included the strategic consolidation of systems and virtualisation of the server estate. We also recommended a shared enterprise architecture to reduce duplication of hardware, software and support resources, and to provide a more efficient computing environment. With any proposed strategy, measurable outcomes are hard to quantify, but we identified significant tangible benefits.

In particular, many of HKPF's systems were out of support and needed to be replaced in the near future. If the force developed these on a like-for-like basis, the costs would be much higher than those for the proposed shared virtual infrastructure – 37% higher according to costs calculated with HKPF. In total, the implementation of the recommended projects aimed to bring about an estimated one-off cost avoidance of over HKD750 million (GBP60 million) between 2015 and 2020.

masonadvisory

Contact us

If you would like to discuss how we can support you please email contact@masonadvisory.com or call +44 (0)333 301 0093.

www.masonadvisory.com