# Security for Police and Justice Organisations

**Business challenges: digital responses**

# Security for Police and Justice Organisations
Business challenges: digital responses

## Policing Today

*"Policing is increasingly concerned with the risks faced by the vulnerable, the threats posed by the dangerous and reducing the harm caused to the former by the latter."*

**- The Police Foundation**

### Changes in demand patterns; drivers of these changes; changes to funding and investment.

The recurring theme here is change, creating a perfect storm of increase in demand, change in the nature of demand, change in the role of police forces and constraints on their resources.

Readiness for change is therefore a critical capability; one that police forces already possess and continue to develop. However, investment in readiness for unpredictable change is hard to anticipate. Understanding common and recurring themes, requirements and 'use cases' informs investment decisions, the most enduring of which are typically made in general-purpose platforms as enablers of flexible, interoperable, secure and collaborative operations that survive the turbulence of today's business environment.

The following highlights are based on our on our extensive research on evolving demand and response patterns in policing:

1. Overall reported crime has increased by around 40% since 2013, with arrest, charging and conviction rates decreasing
2. Crime rates for 'traditional or 'volume' crime types (e.g. robbery, theft from the person, violence) have been increasing sharply after a long period of decline
3. Crime rates and the complexity of emerging crime types (e.g. cybercrime, human trafficking) significantly higher to 'traditional' and increasing - as are the resources needed to process them.
4. Demand for Police safeguarding (managing 'high harm; crimes) is rapidly increasing
5. The ratio of crime cases to number of officers and staff has increased by some 43% since 2013.

### As we all know, these changes are driven by several influencers including:

- the Internet,
- international mobility
- criminal digital capability
- serious and organised crime
- social fracture and disintegration.

### Staffing, funding and investment are also changing, leading to a focus on:

- upstream intervention
- evidence-based investment approval
- 'top-slicing' of force budgets
- headcount reduction
- 'cost shunting' as cuts to other areas of public spending are passed onto policing as first line of response.

# Security for Police and Justice Organisations
Business challenges: digital responses

## Seven Business Challenges

Based on research at market level and with individual forces, we have identified a key set of recurring business challenges common across all forces regardless of local variations (e.g. geography, social or cultural mix, scale, demographics, operating model and history. For all these, digital security is a critical enabler of the response.

These are, by no means, the only or even the most significant challenges (e.g. funding, demand changes), but are the most common and significant challenges across all forces irrespective of drivers of variation, e.g. geography, social mix, scale, operating model:

1. **Place-based Multi-Agency Local Teams and Hubs.** Complex crime, complex social systems and effective interventions increasingly require co-working across geographically based agencies such as Police, Fire, Ambulance, Healthcare, Social Care, Housing.
2. **Officer, Workforce and Citizen Mobility**. significant factors include: the need for visible community-based policing, pressure on real estate, 'real-time' administration (e.g. system-of-record form filling and evidence collection) and multi-agency co-working. Mobile devices deliver tangible, often mission-critical benefits.
3. **Multi-Force Regional Operations.** Geographically related forces will intensify their joint operations focused on interoperation through interoperation standards and the tactical sharing of resources (e.g. people, premises, etc).
4. **Sharing Services and Capabilities.** More forces are sharing common services and capabilities for convenience. Opportunities to do so are increasing particularly in the areas of support services such as digital/ICT HR, and specialised services (e.g. forensics, cybercrime), with significant opportunities to combine force capabilities and deliver economies of scale.
5. **Diversity and Investment in Devolved Environments.** Each force is increasingly managing a diverse range of systems that are either: owned and managed; shared with adjacent forces and agencies; sourced nationally. The result is operational pain due to digital incompatibility.
6. **Cyber Crime and Digital Sophistication of Criminals.** Rapidly increasing incidence of Cyber Crime and the exploitation of digital technology (and vulnerabilities) by criminals requires forces to be 'one step ahead' in the digital arms race and digital evidence collection.
7. **Digitisation of Workflows and System of Record.** Easing the administrative burden on front-line officers and automated collection of evidential-quality information (including media and structured data) is a critical constraint on the ability to 'do more for less' and hand off cases to justice and case management processes in a physically distributed environment.

Read Police and Justice: The Business Security Challenge for more on this

# Security for Police and Justice Organisations

Business challenges: digital responses

## The Digital Response

The police and criminal justice sectors are looking to take advantage of the digital revolution in order to keep pace and deliver effective policing in a world where digital technology takes an ever-increasing role.

Delivering digital capabilities that address the business challenges places significant demands on the underlying network. These require that some of the legacy models of delivering security evolve from a purely boundary-based, defensive approach to one that improves in visibility, adaptability and operational security practices for a more dynamic, business-enabling architecture

Unfortunately, in many sectors, security is often a siloed activity, applied late to a project lifecycle and often in a negative context, creating the perception that security is a blocker rather than an enabler. This approach results in outcomes that at best mean a project never quite realises its promised benefits. At worst, it can result in opportunities for genuine business improvement being missed altogether.

## Architecting the Security Response

An architectural approach means treating security as an end-to-end system rather than a distinct set of individual components. The overall security system should be integrated, allowing for easier management. At the same time, it should enable sharing of contextual and threat information for a more responsive and effective outcome.

**Guiding principles for this approach:**

- A policy shift where security is a business enabler
- Acceptance that it is no longer a case of if, but when a security breach occurs
- Security must focus on improving detection and remediation times, in addition to protection
- Security should be developed as a system – distinct components should not operate in isolation but integrate to improve manageability and deliver more accurate threat detection.

This business-driven method must first identify the information assets, systems and services that support the business, to assess the impact of compromised assets.

**Building clear traceability between business objectives and security helps to establish:**

- Clear justification for security investment
- Which business objectives are at risk due to controls not being in place
- A roadmap from current to target state
- An environment where security is designed-in from the outset.

We believe the following key security capabilities make the most significant response to business challenges and successful delivery of the overall policing mission.

# Security for Police and Justice Organisations

Business challenges: digital responses

## Network segmentation

The ability to divide a single physical network in to distinct logical zones is not a new concept, but it is a fundamental enabling capability. It varies in its transparency and ease of use and must possess the following characteristics:

- **Dynamic–** co-located teams will be made up people from multiple agencies; the network must be able to identify, authenticate and apply control to users and devices from each community.
- **Consistent –** enforcing segmentation at only one point in the infrastructure is insufficient. The technology must be able to support end-to-end segmentation across both the local and wide area network
- **Manageable –** dynamic segmentation approaches have traditionally been difficult to administer, placing significant operational demands on IT support staff.
- **Transparent –** the most effective security controls 'just work'. They are designed in from the outset and delivered in a way that simply enables users to perform their job function.

Dynamic network segmentation relies on a robust identity platform to authenticate users, devices and permitted access levels. A centralised Identity and Access Management platform (IAM) that enables secure, flexible working across UK policing is a must, one example being the National Enabling Programme (NEP).

Such platforms can underpin any network segmentation strategy for a consistent 'single source of truth' that grants users and devices access to the systems required, regardless of location.

## Visibility

As organisational and operational barriers are removed, there is a corresponding increase to the overall risk. This new, shared environment can no longer be protected (or constrained) by a simple, defined security perimeter. Information flow and user mobility demand a more open environment, meaning that this perimeter becomes almost impossible to define and control effectively.

Building assurance in such an environment depends on building visibility-enabled trust and confidence – everywhere. The network is in a unique position to deliver this as flow recording sees all traffic flows from all applications on all nodes and devices. Metadata captured from every conversation on the network includes characteristics such as the conversation endpoints, the protocols used to communicate, and the volume of data transferred in each direction, without needing to capture the actual content of the flows.

Network flow monitoring enables establishing a 'normal' baseline against which to identify undesired and malicious behaviour, including:

- excessive one-way data transfer – which could be evidence of data being stolen
- data being transmitted between systems, which should not be permitted.

Metadata analysis also helps to address the challenges presented by encryption. The past few years have seen significant increases in the use of encryption protocols by the hacker community, in order to hide nefarious activity.

This leaves defenders with the difficult task of separating the good from the bad, plus the practical challenges of resource-intensive decryption.

# Security for Police and Justice Organisations
Business challenges: digital responses

## Secure mobile working

As forces routinely use mobile devices for operational, back-office and mission-critical purposes, they must be subject to robust controls to ensure that they remain useable and effective front-line policing tools. They must also deliver the platform integrity needed to enable evidential quality data collection.

Mobile devices will often use untrusted networks such as 4G or open Wi-Fi; distributed applications requiring access to force-hosted systems must be protected whilst in transit, as must their data.

To deliver maximum usability, this secure connectivity must exist by default and be able to cope with changes to underlying connectivity as devices roam from one medium to another (e.g. VPN), carrying all traffic back to the force hosts. Another option involves selecting specific application traffic for this treatment, with other traffic being allowed to access the Internet directly from the mobile device.

The mobile endpoint itself also needs protection. Malware remains an ever-present, sophisticated and high-volume threat, exploiting any weakness that may be present on an endpoint.

**Endpoint anti-malware solutions should provide:**

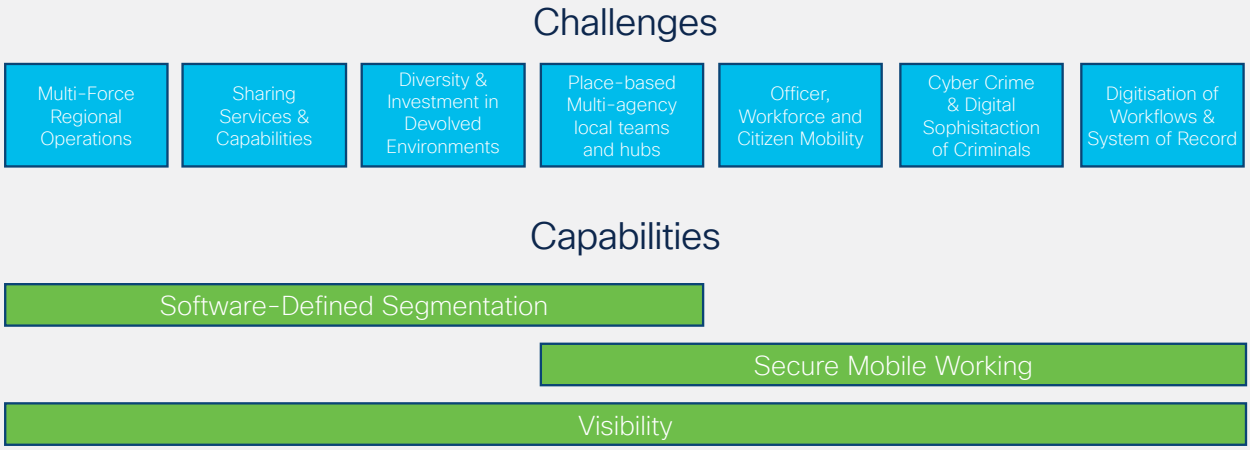
- Support for detecting and preventing advanced threats, including file-less malware
- Consistent support on a wide range of mobile platforms such as Microsoft, Apple MacOS and iOS as well as Google Android to improve visibility and provide a consistent level of protection.
- Retrospective protection; sophisticated evasion techniques can allow malicious files to initially appear benign, only to cause harm later.

## Summary – the benefits of an architectural approach to security

Police and justice organisations face several diverse and complex business challenges. Digital security has a vital role to play in addressing each one Adopting an architectural approach to the planning, design and implementation of these digital security capabilities can deliver significant benefits, increasing effectiveness and reducing complexity.

The three capabilities outlined above represent those that can make the greatest contribution towards addressing the challenges we've identified. The implementation of any single holistic capability has a significant impact on multiple business challenges. This means that 'platform' economics apply – investment in any one capability generates a return against many business challenges.

## Justice Digital Security Capability Mapping



**Security for Police and Justice Organisations**
Business challenges: digital responses

## Continue the conversation

Contact Mark Jackson, our Principal Information Assurance Architect – UK Public Sector

Cisco UKI Justice

Cisco.co.uk/security

Download the infographic

Read the E-book