**Performance and Resources Scrutiny Programme 2018/19**

**Report to: the Office of the Police, Fire and Crime Commissioner for Essex**

|  |  |
| --- | --- |
| **Title of Report:** | **IT QUARTERLY REPORT – UPDATE ON INFRASTRUCTURE MODERNISATION** |
| **Chief Officer** | **Mark Gilmartin,** **Director of Support Services** |
| **Date Paper was Written** | **16th July 2018** |
| **Version Number** | **1.0 - Final** |
| **Report from:**  | **Essex Police & Kent Police** |
| **Date of Meeting:** | **26th July 2018** |
| **Author on behalf of Chief Officer:** | **Jules Donald, Head of IT Services** |
| **Date of Approval:** | **17th July 2018** |

1. **Purpose of Report**
	1. To brief the OPFCC on progress made over the last two years to the Essex Police and Kent Police IT joint infrastructure platform (including data centre servers and databases, data storage, networks, internet, email, end user computing/EUC devices and application rationalisation), and inform on some of the benefits that this has brought to Essex Police, including reduction of organisational risk and some significant service improvements for police officers and staff.
2. **Recommendations**

2.1 For the Committee to note the update and give any feedback.

**3.0 Background**

3.1 **Legacy Inheritance post Essex and Kent Initial IT Convergence**

An independent landscape review of IT for both forces was commissioned by the incoming Chief Officer for IT (Mark Gilmartin) in 2015, which highlighted a number of organisational failings in IT provision for both forces, including historic under-investment in the infrastructure and a high level of over-engineered legacy complexity. This was starting to create a number of critical issues, including;

* Regularly slow-running and failing IT systems holding critical policing data
* No consistent guarantee of access to data back-ups when systems failed
* Daily customer frustration with a poor user experience in terms of speed of booting up computers and slow email performance
* Challenge for IT Services in speed of troubleshooting and restoration of service due to complexity of legacy landscape ‘knitting together’ of systems and lack of standards and design documentation
* Inability to patch a number of old systems and servers (no longer supported by the manufacturers) creating cyber security vulnerabilities

Reflecting the impact on operational and organisational performance, these issues culminated in three interdependent risks on the joint force risk register:

* URN 1241 – strategic level - the unreliability of the IT infrastructure platform causes detrimental impact to operational policing delivery
* URN 1001 – management level - vulnerability to Cyber Security attacks, due to age of infrastructure and lack of modern defences
* URN 1559 – management level - our accreditation to continue accessing the PSN network would not be approved, due to the vulnerabilities in our infrastructure creating a risk for other organisations

**4.0 Executive Summary**

4.1 **Fast-Track Infrastructure Modernisation (FIM Programme)**

In response to the review, a significant change and investment programme was initiated for IT Services by the Head of IT in 2015/16 after the independent Methods review of IT Services, culminating in three phases of infrastructure modernisation for both forces.

**Phase 1** concluded successfully in March 2016, and produced a number of immediate governance, process and structural improvements, including; an IT service operating model, an IT strategy, a stronger governance model for budgetary control, a revised management structure, technical architecture standards, and a much improved control on software licensing compliance, including a new 3 year enterprise agreement with Microsoft and an agreement with SAP. Documentation on phase 1 has been previously circulated to both Chief Officer teams and OPCCs, so this report focuses on the achievements in phase 2 over the last 2 years.

4.2 **Phase 2 Budgetary Provision**

Since the initial phase 1 investment which prioritised process change and software licence compliance, subsequent FIM investment has been via the annual PFCC/PCC approved Essex and Kent investment programme, in what was formerly known as the IT rolling replacement budget, or technical refresh. FIM funding for the last 2 years is summarised below, with 3 original budgets merged into 1 FIM technical refresh budget from 2017/18:

|  |  |  |  |
| --- | --- | --- | --- |
| FIN YEAR | ESSEX | KENT | TOTAL |
|  | CAPITAL | REVENUE | CAPITAL | REVENUE |  |
| **2016-17** |  |  |  |  |  |
| Servers | £487,000 | *Not available* | £487,000 | *Not available* |  |
| Networks | £100,000 | *Not available* | £200,000 | *Not available* |  |
| EUC Devices | £185,000 | *Not available* | £230,000 | *Not available* |  |
| **2017-18** | £1,575,000 | £81,000 | £830,000 | £51,000 |  |
| **2018-19** | £3,261,000 | £491,000 | £2,590,000 | £491,000 |  |

*NB: - in 2016/17, the annual replacement budgets were still reduced as a result of comprehensive spending review impact, but from 2017/18 onwards, the realistic cost of maintaining the infrastructure has been factored in, hence the significant budget increase requirement.*

*The higher Essex figures reflect the previous under-investment in the Essex infrastructure estate, and the pressing need to replace the platform.*

**5.0 Current Work and Performance**

This report gives a progress update on the key areas of FIM as below, and outlines some of the immediate benefits. It should be noted that the majority of benefits are associated with productivity and efficiency improvements, corporate risk reduction, performance improvements and improved enabling services for digital transformation, so financial savings are not prevalent. It is anticipated that from 2019/20 onwards, the standardised improved infrastructure costs should reduce in some areas (eg. on premise data storage), but this will be counter-acted by a gradual move to hosted services and cloud storage, with a shift in expenditure from capital to revenue (and a higher revenue proportion already seen in the 2018/19 budget requirement).

**5.1 End User Computing Devices and the Microsoft Windows 10 Operating System**

A big improvement in the last 2 years has been the deployment of Mobile Smart Phones, light weight laptops and the development of the Windows 10 solution, which has really helped the two forces move towards an agile working culture.

**Mobile Smartphones** - the deployment of the Mobile devices has enabled users across both organisations to migrate from older phones to over 4,400 modern Samsung smart phones used by the Mobile First police officers and a range of managers, enabling them to access police IT systems and data while out on shift or from home. The recent integrated software platform from HCL application is already giving multiple benefits in reduced time for officers, with a single point of search and a reduction in the need to copy data from one app to another using better workflow, and IT Services played a key role in implementing this service into our systems and infrastructure.

**Agile Laptops** – 341 lightweight Lenovo 2 in 1 Thinkpads have been rolled out to senior managers and officers, with much positive feedback about the speed of connection and how easy, flexible and light the devices are to use. Following this positive response, further lightweight Dell 2 in 1 laptops are currently being procured for deployment across Kent and Essex to other support staff.

We are working with a number of teams within SCD (SOCU, Intel) and Major Crime to replace workstations with Windows 10 laptops and agile devices. This is enabling agile working for detectives within these areas and being well received as a real improvement in their operational capabilities and reduction in downtime when, for example, waiting around during court appearances and deployed on enquiries. This is avoiding growth due to recovering both their workstations as well as previously shared laptop devices

In parallel, we have recovered a substantial number of legacy iPads, with a reduction in the associated support overhead. Additionally this has enabled revenue savings of approximately £10k p.a. from the cancellation of the associated iPad data sims (the Windows laptops are only configured for wifi or tethering connections as a cost saving initiative).

This year’s FIM budget will enable more of the above with the introduction shortly of the new Dell 2 in 1 tablet (Yoga style equivalent). We will start to see more of a reduction in our traditional desktop estate, except in key static locations, as we enable more agile capabilities.

**Windows 10 Rollout** – IT Services spent over 10 months developing a secure build for the new Microsoft Windows 10 platform, ahead of the national NEP (National Enabling team) programme design, which has been based on our work. This has involved over 2,000 NCSC (National Cyber Security Centre) defined elements of configuration to make our computing devices secure to use on the police network as opposed to a commercial model. The positive benefits of using Windows 10 as opposed to the legacy Windows 7 build is a much improved performance for our users, particularly when logging in in the mornings and accessing applications throughout the day. **It is estimated that on average a member of police staff gains over 30 minutes a day in improved productivity as a result of Windows 10, which also helps with email performance.** Windows 10 also offers much greater security protection against cyber attacks, and is the platform required before we can migrate to the Office 365 platform.

IT Services are working hard to migrate both force’s computing estate of over 12,000 devices from Windows 7 to Windows 10 - we have now reached 50% of workstations as a whole, including a 70% workstation target in Essex. The laptops are proving more challenging due to different incompatible legacy applications, but a third are now migrated. Completion is targeted for September 2018.

**Email Performance** - we have significantly improved the stability and performance of email in the last year, in parallel to working towards the goal of Office 365 and migrating our on premise email solution to Exchange Online as well as many of our Microsoft services to the cloud. This is radically innovative across policing in the UK, and Essex and Kent are the two pilot forces for O365 NEP programme, and have been key contributors to the development of the solution for policing. Currently 50 users from IT have been migrated to the cloud, and we await further support from the NEP to continue the rollout.

**5.2 Date Centre, Data Storage and Server Improvements**



Over the past 2 years we have laid the foundations and created the Infrastructure building blocks that move us to a modern infrastructure platform. The previous years’ investment has already started to see dividends in 2017/18, with a new three tiered storage environment, as shown in the diagram above, with further detail below:

* The platinum Nutanix platinum infrastructure is hyper converged (super resilient and highly available and is a virtualised environment) and has started to run our blue light critical systems for both forces, including Genesis and ARC in the FCR
* Work is already in planning to redevelop STORM, SAP and REDBOX underlying infrastructure platforms. CITRIX technology will pave the way to the removal of NETC (the old confidential network) and all its legacy infrastructure.
* A Gold FX virtualisation platform (in essence 8 servers per force and 500TB of Compellent storage at each site) in the CDC (Chelmsford data centre) and MDC (Maidstone data centre) will house all non-Platinum systems that can be virtualised and that are not a legacy system.  This is now commissioned and running,
* SAP will see 3 racks of physical hardware going and replaced with half a rack of hardware which will also run many other systems as well
* The ICCS hardware is in and we are moving forward to support APD in the first stage of testing
* Storage - Isilon storage was commissioned on 31st January this year giving the force an enterprise class media storage solution, which will house data like Redbox voice recordings, Drone footage and any other media requirements for both forces.  This is well underway with a view to standardise all storage on this platform. This has been further aided by the provision of our new 40GB data links (WAN) between both forces giving us ample room to migrate and replicate this data whilst ensuring a high quality service for all our staff across each county
* CommVault backup solution (stage 1) Backup for both Platinum and Gold and Silver infrastructure – this was commissioned in June 2018 to resiliently store all backups of critical systems
* Bitdefender - new server specific Anti-Virus and Anti-Ransomware protection due to be up and running protecting 1400 servers by July 14th 2018
* Ivanti patch management suite - will help deploy the latest security patches, manage and where possible automate the process, In and testing go live August 2018 (patching policy now approved in both forces
* Migration and in house provision of IT services to Kent TSU
* Digital Forensics (DFU) new storage solution 280 TB of storage to hold and search evidential data ready for case prep (Jan 2018)
* O365 Infrastructure in and ready for migration (November 2017)
* Genesis migration October 2017

**Next steps for 2018/19 include:**

* A Bronze virtualised  server environment being built in Folkestone data centre ready to migrate off our aging hardware (NetApp, Old SAN, legacy VMware for both forces), this will remove old out of warranty hardware, its upkeep and bring the virtualisation environment back onto a supported version - October 2018
* Modular Datacentre CDC remediation, a modular container server room solution to give Essex a fit for purpose economic environment that is able to cope with demands of a modern datacentre – planned for late October 2018
* Commission Data links and ensure Network availability in Folkestone which will house our d ECS storage site and creation a Bronze server location
* ECS storage (Elastic Cloud Storage) - 1 petabyte will house all our unstructured data - this will live across 3 locations (MDC.FDC,CDC) making is highly resilient with cloud ready capabilities, install and commission for October 2018
* Our new Bronze legacy virtualised environment will help protect us from any security holes often found in aging legacy operating systems and any lack of vendor fixes due to them being end of life.  This work will include firewalling off Bronze from our Gold and Platinum environments, only allowing those that require access or connection,  archiving of systems,  updating to the last available patch, removal of all ‘no required’ programs, no access to the PSN or internet.  All migrated to in warranty hardware. Staging move to Folkestone October 2018
* Legacy systems and decommissioning (Essex and Kent) - on average we are migrating or decommissioning 3 servers per week since November 2017
* DMZ (Demilitarized Zone) redesign of how we connect out to the cloud and 3rd party organisations, the public and receive data back into our datacentres – work starts June 2018
* Nessus Vulnerability scanner - real-time scanning against our server environment looking for vulnerabilities, once found we can patch and remediate proactively
* We are also implementing a new platform called Oracle Database Appliance. This is required to replace the ageing platforms of our operationally critical Oracle based systems such as Storm. This will form the 'core' of these systems around which the application tier will then be modernised. This will be a complete Oracle engineered High Availability solution based on Oracle hardware and software which has been optimized by Oracle for maximum performance and resilience based on its flagship RAC technology. This will bring technical consistency to the way these systems are managed in both Kent and Essex and will benefit from, amongst other things, Oracle Premium support and bundled patching technology.

**In summary** - much work has taken place to design, replace and build the majority of both forces’ legacy server and storage platforms with modern, resilient solutions enabling smoother performance, decreased risk of failure, and secure back-up of data on systems in the event of failure. This also facilitates our data and applications to be transferred to cloud storage in the future. There are also important improvements in removing legacy unpatched servers, investment in proactive anti-virus scanning and monitoring systems, helping reduce our risk re cyber security attacks, and improve our PSN accreditation risk score process.

The ultimate benefit of this investment (in addition to reducing risk on the likelihood of a cyber security attack) is the improvement in the reliability of our IT systems and the benefit this gives to accessing operational data required continually for front-line policing purposes – this detrimental impact of system failure has been demonstrated on numerous occasions over previous years with incidents impacting FCR systems, email performance, Codes data, Op Vitrix, Genesis data access and many more.

This work has been overseen by our third party data centre experts, Softcat, to assure that the solutions we are implementing are industry best practise.

**5.3 Network Improvements**

* Streamlining of our Network support contract - by looking at our single biggest service provider, BT, and identifying other functions we were using different third parties for, but which BT could have been providing, several contracts were renewed under BT, or novated across to BT. A new agreement was drawn up whereby we agree to use BT in the future if possible. However, they do still need to remain competitive, and if not, we have clauses in place allowing us to direct BT to subcontract to the cheaper third party when required. This piece of work has saved approximately **£1.2million over 5 years**, which has been given back through finance. It is an ongoing practice to review our support arrangements to ensure that they offer best value for money combined with an appropriate level of support for the organisation as the technological usage changes.
* Nexus 9k data centre work - we have installed new Cisco infrastructure to underpin the modern server and storage facilities in our data centres in Chelmsford and Maidstone, and soon, Folkestone. The best practice method uses a spine and leaf approach to provision networks links across the data centre and allows us to manage the security of our internal network more flexibly than was previously possible. This has been configured with expediency in mind initially, to facilitate the other IT teams to do their work, but is a future-looking scalable solution for our internal security that we will be able to adjust and adapt for systems’ varying security requirements.
* WiFi update - We are replacing our older Ruckus WiFi Access Points (APs) with new Cisco Meraki equipment and co-ordinating this with the replacement of the ECIS Guest internet access. The 7 force preferred public sector WiFi option is GovWiFi. Kent County Council use GovRoam, a similar methodology, so we are accommodating both in certain locations at present. This work is ongoing, but we have installed the management servers required and are proceeding through a 4 year roll-out plan to replace all Ruckus APs with Cisco APs and ultimately expand the WiFi coverage that we have across both organisations. This will allow for maximum use of Mobile First project technologies.
* 10GB links between Data Centres - we have linked the data centres in Maidstone and Chelmsford with a 10GBit link, which is making the operational experience of systems that use internal traffic much smoother. This has enabled Microsoft Exchange to be used more reliably, and will allow for increased traffic from other systems to be implemented without degradation in application response times. For internal IT, this has improved the response times and performance of many tools and bulk copying facilities, such as backup taking, where the files have needed to be passed from one datacentre to the other for resiliency and security purposes. Previously these kinds of things would have taken much longer and prevented engineers moving on to other work. This will give us additional security and resiliency, as well as a new level of flexibility when it comes to hiving off legacy systems prior to their shut down.
* Cloud-based services accessed via the public internet – with the increase in cloud-hosted policing services accessed by the internet through our environment as a gateway, it is a key priority for IT Services this year to ensure that the bandwidth of our access points at the external firewall is sufficient. Much work is currently being undertaken with BT to measure the likely impact and required technology changes to enable solutions such as Axon BWV and Office 365 productivity services.

**5.4 Application Rationalisation**

There are over 160 different operational applications in existence across the Essex and Kent IT estate – which drives a number of challenges, including duplication of data and business process functionality, increased cost and effort in terms of support (both for internal IT staff and external non-pay budgets), and of course the security loop-holes in legacy systems that are not kept up to date in terms of updates/patches by the original providers, but are still in use operationally. The need to rationalise a large number of our legacy systems is intensified by force responsibilities to be compliant with legislation such as MoPI and GDPR.

* A project was commenced in 2016 to look at how we can best start to streamline and rationalise our many legacy systems.
* We have progressed well with ‘tactical application rationalisation’, eg the systems which we have a vested interest in decommissioning due to PSN non-compliance, hardware issues, etc.
* Systems decommissioned in recent months include the legacy ANPR JetBOF, CTIU CLIO, CrimeBOS, EPOS, KIM Custody, Maxbridge Asset Management, Optica, PredPol, STOPS and SWARM. Systems earmarked for decommissioning in the coming months include Agresso, Locard, Promat 2, Sea Eagle, Solcara, Surveybook and Video Witness.
* The longer-term strategic approach is to use the Data Library as a one-stop shop for legacy data with a single point of search. A business case for this solution is underway in Essex, with ongoing supplier consultations on the best type of solution. Successful delivery of this will enable us to decommission approximately 5 more systems including pre-Athena legacy applications for Essex, and opens the door for more to be decommissioned in future when we have a requirement to retain access to the data.

**6.0 Implications (Issues)**

**6.1 Links to Police and Crime Plan Priorities**

The improvement and future-proofing of the force’s IT infrastructure platform enables and supports all the key elements of the PFCC’s Police and Crime Plan priorities – as effective policing and communication with the public is dependent on smooth-running technology. Most specifically, the infrastructure work either directly or indirectly supports the objective around ‘Effective use of Technology, enabling:

* Mobile policing to frontline officers (Mobile infrastructure and smart phone devices)
* Strengthening our ability to share data and intelligence across partner agencies (Office 365 and Athena)
* Effective delivery of the Athena IT system – the local infrastructure providing the access to this operationally critical system

**6.2 Demand**

Whilst not directly applicable, the improvement of our technology platform enables the smooth-running of a number of critical systems in the Public Contact and Force Control Room environment which are crucial to managing and reducing demand.

**6.3 Risks/Mitigation**

Our force risks for IT infrastructure, Cyber Crime and PSN Accreditation are reducing in terms of scores and levels of mitigation required, and are regularly reviewed by the Deputy Chief Constable in his quarterly star risk chamber session:

* URN 1241 – **Failure of our IT Infrastructure** – commenced in January 2017 at a score of 100 (almost certain/catastrophic), currently at 20 (possible/major)
* URN 1001 (1458 closed/merged with this) – **Cyber Security Attack** – remains at a score of 20 (possible/major)
* URN 1559 – **Risk of Achieving PSN Accreditation** – remains at score of 15 (probable/significant) due to the national accreditors NPIRMT not having capacity to have reviewed our 2018 submission as yet – but realistically this risk is likely to reduce due to FIM progress made, as already acknowledged by NPIRMT in their assessment of our Office 365 readiness

As demonstrated in this overview, much progress has been made in stabilising our infrastructure platform and providing better access to police data in the last 2 years. This includes the patching of our computing device and server estate, remediation of legacy servers, the implementation of new tiered storage with greater resilience, proactive anti-virus monitoring tools, a new computer operating system (Windows 10), new agile devices, creating a platform that prepares us for cloud migration in the future of older systems, and reduction of some old security-flawed applications.

The benefits of the new platform are already apparent, with generally a much quicker and more stabilised user experience when accessing police IT systems – this is evidenced by the Priority 1 (critical fault impacting one or more users from conducting their role) fault report reduction shown over the last 2 years:

* 2016 – 827 reports
* 2017 – 843 reports
* 2018 – 199 (first 6 months)

**6.4 Equality and/or Human Rights Implications**

Not applicable

**6.5 Health and Safety Implications**

 Not applicable

**7.0 Consultation/Engagement**

* Various IT technical staff
* Various IT external partners, including Softcat, BT, Microsoft, Risual and Methods Advisory
* Paper circulated to:
* Essex and Kent Joint Chief Officer Group – 26th June 2018
* Quarterly Strategic IT Steering Board – 17th July 2018 (including OPFCC attendance)

**8.0 Actions for Improvement**

IT Infrastructure Modernisation will remain an ongoing priority for IT Services, as we can never be complacent around the advances in cyber crime attacks, and it is vitally important to maintain our technical infrastructure environment and maximise the advances of new types of technology to protect our valuable asset of electronic policing information. To this effect, while the final year of FIM improvements will be complete by March 2019, the ongoing IT technical refresh annual capital investment budget will continue to provide the updates and improvements required for the future.

A key requirement from HMICFRS is for all forces to have an ambitious digital transformation plan in place by September 2018 – this is being progressed in Essex alongside an exemplar guide forthcoming from Commissioner Ian Dyson & IMORCC. The work of the previous years (and ongoing) in stabilising our IT infrastructure platform is critical to the delivery of digital transformation initiatives for Essex Police.

**9.0 Future Work/Development and Expected Outcome**

The IT Services annual business plan (2018/19) demonstrates the advances planned for this year in technical refresh – and the forthcoming stage 1 capital business case for Tech Refresh 2019/20 will lay out further detail of technical development. In terms of benefits to Essex Police, the positive impact of FIM is being incorporated within the current Operational Benefits workstrand in Corporate Services.

**10.0 Decisions Required by the Police, Fire and Crime Commissioner**

None at this stage – the paper is for information ahead of the next capital submission for 2019/20 technical refresh.