NOTTINGHAMSHIRE
Fire & Rescue Service
Creating Safer Communities

Nottinghamshire and City of Nottingham
Fire and Rescue Authority
Finance and Resources Committee

ICT STRATEGY UPDATE

Report of the Chief Fire Officer

Date: 19 January 2018

Purpose of Report:

To update Members on the progress of the ICT Strategy and the progress made in improving the information and cyber security of the Service.

CONTACT OFFICER

Name :	Craig Parkin Assistant Chief Fire Officer
Tel :	0115 8388100
Email :	craig.parkin@notts-fire.gov.uk
Media Enquiries Contact :	Therese Easom (0115) 967 0880 therese.easom@notts-fire.gov.uk

1. BACKGROUND

1.1 The Information and Communications Technology (ICT) Strategy for Nottinghamshire Fire and Rescue Service (NFRS) was produced in response to the Strategic Review of ICT in October 2012 and the Information and Communications Technology Strategy Report produced in February 2013 produced by Cronins on behalf of NFRS.

1.2 The strategy provides a clear direction for NFRS, supported by the operational and strategic goals of the Service and the Strategic Business Requirements (SBRs) provided by Cronins.

1.3 The ICT Strategy 2013 document summarised both the state of ICT within the Service, in the form of a gap analysis, highlighted risks in ICT and provided a clear direction for improvement in ICT provision.

1.4 The overall aim of the ICT Strategy for Nottinghamshire Fire and Rescue Service (NFRS) ICT Strategy was to achieve a balance of organisational efficiency and new innovations:

"To reduce organisational risk by creating a foundation of ***standardised***, ***resilient*** and ***integrated*** systems with ***simplified*** processes; delivered by cost-effective ICT services and solutions that are focussed on the needs and objectives of Nottinghamshire Fire and Rescue Service."

1.5 In April 2016, the Finance and Resources Committee report 'Information and Communications Technology Strategy 2016' provided Members with an update on the progress of the Information & Communications Technology (ICT) Strategy 2013.

1.6 The report outlined that the ICT Department had delivered against 92% of the 2013 'Strategic Business Requirements' targets, and 77% overall targets of the 2013 Strategy. Members were also briefed on the delivery of £173,000 of revenue savings, achieved by reviewing the ICT budget and supplier contracts.

1.7 The report also outlined the Service's proposed approach to ensure that it continues to provide an effective ICT infrastructure, to meet its information management and IT security responsibilities until 2020, with focus on four connected work streams including:

- Unified collaboration;
- Unified communications;
- Connected workforce;
- Emergency Services Network.

2. REPORT

2.1 This report updates members on the progress being made on the ICT strategy, how demands and risk are changing and makes recommendation as to how the Authority ensures that future demands, threats and resulting risk are appropriately managed. Work on the strategy has also involved changing the culture within the ICT department, moving towards the principles of IT as a Service (ITaaS), as characterised in the following areas:

- Making a positive contribution to drive through transformational change to improve NFRS;
- Customer focused and striving to deliver excellence to meet the needs of the service and empower staff to make best use of their ICT facilities;
- Embracing appropriate innovation with demonstrable value for money;
- Increasing the resilience of the ICT infrastructure.

2.2 As part of the review of the ICT Strategy 2016, the four connected programmes of work streams have been examined to demonstrate where progress has been made against each area, with examples such as:

- **Unified Communications** - the implementation *of* Skype for Business was completed in March 2017. This has been followed by some smaller projects to ensure that the Service is realising the potential of the system, for example the proviso of web-cam monitors across the Service to facilitate easier communications using Microsoft Skype for Business and Microsoft Surface Hubs installed at HQ, SDC and Highfields;
- **Unified Collaboration** - progress in delivering against this work stream is scheduled for be completion by the end of 2018, including an updated SharePoint infrastructure, a new NFRS website launched in December 2016 and a new NFRS intranet launched in November 2017. Future products include an extranet scheduled for March 2018 to facilitate multi-agency collaboration and the new electronic document and records management system is scheduled to be live by December 2018.
- **Connected Workforce** – projects have already been delivered within this work stream that enable employees to better deliver services, including an upgrade to CFRMIS to enable access to an Operational Intelligence module to be provided for operational crews. The Service now benefits from upgraded mobile devices, the latest version of Microsoft Office 2016 and migration of the email system to Microsoft Office 365 has commenced and should be completed by March 2018.
- **Emergency Service Network** (ESN) – progress in delivering against the Emergency Services Mobile Communications Programme (ESMCP) is

reported into the Policy and Strategy Committee, however several internal 'cyber-security' projects are being managed by the ICT Department.

These include, Public Sector Network (PSN) Information Technology Health Check (ITHC) completed by an external supplier November 2015, this created a baseline of security vulnerabilities to enable the NFRS ICT Department to measure progress against the project to improve the cyber-security of the Service. Also, the IT Security Officer has commenced the application process for the Service to become Cyber Essentials Plus certified; to improve our defence against the most common cyber threats and demonstrate the commitment of the Service to cyber security. Furthermore, certification will aid the process of gaining Emergency Services Network (ESN) Code of Connection and address other compliance requirements such as the EU General Data Protection Regulation (GDPR).

2.3 The above areas reflect the diversity of projects that are required to deliver modern public services, they also emphasise the complex operating environment in which emergency services are heavily reliant upon technology. This operating environment is a growing area of risk that requires continuous review to be able to identify risk and how that risk should be managed, building the significant commitment and progress since the Authority adopted its current ICT strategy.

2.4 Day to day risk can be seen in the form of cyber-attacks, as recently experienced by the National Health Service (NHS) or the Services ability to mobilise as an emergency service to communities. Over the last 2 years, fixed term contract staff have been recruited to provide the necessary capacity to deliver services, for example, the role of information security officer.

2.5 The current programme of work is continually reviewed and added to, for example, the Services ability to collaborate with other organisations requires systems and capability to do so as a secure and trusted partner, resulting in the development of an Extranet.

2.6 Therefore, it is highly likely access to the current fixed term capability will be required on a permanent basis, this report therefore recommends that officers provide an assessment of future resource requirements for Member consideration in a future report.

3. FINANCIAL IMPLICATIONS

3.1 An earmarked reserve of £250k was previously agreed to support the preparation work for PSN compliance, this is now seeing significant spend and will be kept under review as the Service works through its remediation plan.

3.2 An increase of £195K to the ICT Salary Budget was approved by the Strategic Leadership Team (SLT) on 19th December 2016 on a fixed term basis, to deal with the additional project demand and resources recruited into the

department to ensure the remediation of security vulnerabilities and achieve Emergency Services Network (ESN) code of connection.

3.3 The Home Office previously provided a Section 31 Grant £209k as part of the Services work for ESN in April 2017 months. This is ring fenced to fund ESN related activities and resources recruited to remediate ESN security vulnerabilities and achieve ESN code of connection.

3.4 Several new systems have been procured to significantly harden the cyber-security position of the Service, as detailed in the table below, range from access control, firewall configuration and security event incident management solutions as examples, requiring an initial investment of approximately £80k.

3.5 The ICT Department undertook a comprehensive annual Public Services Network (PSN) Information Technology Health Check (ITHC) in September 2017, that cover penetration testing, security policies and procedures, social engineering audits and vulnerability testing £28k. There is a continued requirement to undertake a PSN ITHC annually once ESN Code of Connection has been achieved, and a revenue budget of £14,000 will be established in FY 2018-19.

3.6 Members should be aware that all the above will require continued funding to ensure the Service is adequately protected from future operational, financial and reputational risk. This report recommends an assessment of the future demands and resources for Members to consider in a future report.

4. HUMAN RESOURCES AND LEARNING AND DEVELOPMENT IMPLICATIONS

4.1 The ICT Strategy, Tri-Service Control collaboration project and ESN continues to place significant demands upon the Service, which has resulted in a number of fixed term arrangements being put in place.

4.2 These have all been delivered within the Service's existing policy framework, but it is anticipated that capacity will need to be maintained on a permanent basis and the longer-term implications of additional workloads that is driven by highlighted risks within this report.

4.3 Consideration of the long-term implications of the hardening of the cyber-security capability of the Service, driven by ESN, are already beginning to highlight additional skill requirements; for example, information security, which is currently being delivered with a fixed term appointment.

5. EQUALITIES IMPLICATIONS

An equality impact assessment has not been undertaken as this report does not amend the current provision of services.

6. CRIME AND DISORDER IMPLICATIONS

There are no crime and disorder implications arising from this report.

7. LEGAL IMPLICATIONS

There are no legal implications arising from this report.

8. RISK MANAGEMENT IMPLICATIONS

8.1 The ICT Strategy is key to proportionality managing organisational risk and this report highlights a sustained and likely increase in risk as the Service transforms over coming years within its financial context and continues to deliver its Integrated Risk Management Plan.

8.2 The Service co-ordinates the management of risk facing the ICT infrastructure through the Security Steering Group that has previously completed a gap analysis against a national Protective Security Framework and good practice. To ensure the Service continues to work towards this level of assurance, it is recommended that the Service assess its longer-term resourcing of ICT to ensure risk continues to be proportionately managed.

8.3 Policy and Strategy committee will be receiving an update for risk management at its February 2018 meeting, seeing the addition of GDPR to the corporate risk register, this will ensure that both committees are provided with a consistent understanding of ICT and Information security risk on which future decisions are to be made.

9. COLLABORATION IMPLICATIONS

9.1 The Service seconds a member of staff for the Tri-Service Control collaboration project, which is currently under review and has resulted in the joint procurement and use of systems to deliver an effective command and control system.

9.2 The head of ICT represents NFRS at the East Midlands Tri-Service Control executive board and acts as regional technical advisor to the East Midlands ESN strategic board and programme, including commitments a t a national level.

9.3 An Extranet capability is being developed to assist with future collaborative opportunities between organisations, initially this will be trialled with the East Midlands National Operational Guidance (NOG) team to ensure they can work

across multiple sites, share information and drive change in operational doctrine.

9.4 Further collaborative opportunities will either be addressed within specific future reports or through the Authority's collaboration strategy, governance structure.

10. RECOMMENDATIONS

It is recommended that Members:

10.1 Note the contents of this report.

10.2 Receive a further report to consider the outcomes of an assessment of risk and resources to proportionality manage identified risk.

11. BACKGROUND PAPERS FOR INSPECTION (OTHER THAN PUBLISHED DOCUMENTS)

None.

John Buckley
CHIEF FIRE OFFICER