From:	**Peter Oakford, Deputy Leader and Cabinet Member for Finance, Corporate and Traded Services**
	Lisa Gannon, Director of Technology
To:	**Policy and Resources Cabinet Committee**
Subject:	**Annual Cyber Security Update**
Classification:	**UNRESTRICTED Report**
	EXEMPT Appendix A/B/C/D - Not for publication – Paragraph 3 of Part 1 of Schedule 12A of the Local Government Act 1972 refers
Past Pathway of Paper:	**Policy and Resources Cabinet Committee – 3 March 2021**
Future Pathway of Paper:	**N/A**
Electoral Division:	**Affects more than 2 Electoral Divisions**

Summary: This report updates **The Policy and Resources Cabinet Committee** on the Council's current approach to cyber security and provides an update to the report presented to this Committee on 3 March 2021.

Recommendation(s):

The Policy and Resources Cabinet Committee is asked to **note** the Council's current approach to cyber security.

1. Introduction

1.1 Over the past year we have continued efforts to secure new systems and processes implemented as part of major change workstreams. These included:

- The progression of Kent County Council's "Cloud First" model of ICT infrastructure.
- Projects to decommission legacy systems, hardware and facilities.
- Response to remote working requirements brought on by the COVID-19 Pandemic.
- Development of hybrid working practices.

1.2 Alongside these programmes, we have responded to an increasing level of malicious cyber activity by improving incident response processes, hardening existing systems and improving our network defences.

1.3 The exempt appendix provides further detail and statistics of these workstreams and how they have improved Kent County Council's security posture.

2. Security Summary

2.1 Cyber criminals continue to take advantage of the global shift to remote working and increased reliance on technology to access public services. Security monitoring conducted by the UK Government's National Cyber Security Centre (NCSC) identified the following emerging trends in 2021:

- A strategic shift to exploiting supply chain vulnerabilities.
- Utilising novel and sophisticated models of ransomware.
- Continuing and increasing cyber activity towards the UK from foreign entities
- Phishing e-mail as the most common threat vector to UK organisations.

2.2 Kent County Council's monitoring activity across its ICT infrastructure suggests that our cyber defences are performing well and recent work to enhance e-mail, firewall and backup resiliency has been successful, which have all been identified by the NCSC as critical attack vectors to be hardened against cyber activity.

2.3 Aside from technical improvements to Kent County Council's e-mail services, we are assessing and improving staff response to phishing attacks, which exploit human error to gain access to systems via fraudulent e-mail. We have launched a series of simulated phishing campaigns to assess staff responses, improve our incident reporting system and to develop training materials to ensure staff are vigilant to the most common cyber threat vector.

2.4 Following completion of testing, the implementation of Microsoft's Security and Compliance (SCP2) suite of applications and services is progressing which will enhance the security of Kent County Council's Cloud-based infrastructure and suitably restrict the sharing of sensitive data. In addition to SCP2's controls, we have increased authentication security and remediated critical zero-day vulnerabilities, such as Log4J.

2.5 The planned technology roadmap activity will incorporate further cloud-based security tools to strengthen resilience against known cyber threats. In order to ensure a secure infrastructure and mitigate current and emerging cyber threats, continued investment in developing security technology must be maintained.

2.6 The Strategic Technology Board and Cross Directorate Resilience Forum has approved a management plan of internal and external audit recommendations related to Kent County Council's technical resilience. Actioning of these plans will further strengthen Kent County Council's security posture and ensure compliance with the relevant external bodies.

2.7 The Authority continues to monitor the ongoing geo-political situation in Russia and Ukraine and is in regular dialogue with the NCSC and National WARP to ensure that The Authority is proactive in its mitigations of increased and related cyber risks. At present, The Authority is aligned with NCSC guidance including implantation of geo-blocking, a resilient backup system, two-factor authentication and anti-malware protections.

3. Recommendation(s)

Recommendation(s):

The Policy and Resources Cabinet Committee is asked to **note** this report.

Report Author:	**Relevant Directors:**
Dave Lindsay Interim Head of Technology Commissioning and Strategy Telephone: 03000 413922 E-mail: dave.lindsay2@kent.gov.uk James Church Interim ICT Compliance and Risk Manager Telephone: 03000 416597 E-mail: james.church2@kent.gov.uk	Lisa Gannon Director of Technology Telephone: 03000 414341 E-mail: lisa.gannon@kent.gov.uk