Agenda No

AGENDA MANAGEMENT SHEET

Report Title:	Proposal for a new all in one Web and Email security platform
Name of Committee:	Emergency Report
Report Director:	Head of Communities and Homes
Portfolio:	Communities and Homes
Ward Relevance:	None
Prior Consultation:	Senior Management Team
Contact Officer:	Jeremy Carter, Corporate ICT Manager jeremy.carter@rugby.gov.uk 01788 533475
Public or Private:	Public
Report Subject to Call-In:	Yes
Report En-Bloc:	No
Forward Plan:	No
Corporate Priorities: **(CR) Corporate Resources** **(CH) Communities and Homes** **(EPR) Environment and Public Realm** **(GI) Growth and Investment**	This report relates to the following priority(ies): ☒ To provide excellent, value for money services and sustainable growth ☐ Achieve financial self-sufficiency by 2020 ☐ Enable our residents to live healthy, independent lives ☐ Optimise income and identify new revenue opportunities (CR) ☐ Prioritise use of resources to meet changing customer needs and demands (CR) ☒ Ensure that the council works efficiently and effectively (CR) ☐ Ensure residents have a home that works for them and is affordable (CH) ☒ Deliver digitally-enabled services that residents can access (CH) ☐ Understand our communities and enable people to take an active part in them (CH) ☐ Enhance our local, open spaces to make them places where people want to be (EPR)

	☐ Continue to improve the efficiency of our waste and recycling services (EPR) ☐ Protect the public (EPR) ☐ Promote sustainable growth and economic prosperity (GI) ☐ Promote and grow Rugby's visitor economy with our partners (GI) ☐ Encourage healthy and active lifestyles to improve wellbeing within the borough (GI) ☐ This report does not specifically relate to any Council priorities but
Statutory/Policy Background:	None
Summary:	The purpose of this report is to propose the purchase and implementation of a new all in one Web and Email security platform.
Financial Implications:	Financial implications are outlined in the body of the report.
Risk Management Implications:	The report highlights the Council's current inability to identify and report on its email and web usage, and the visibility and control of threats targeting the organisation originating from these sources. Furthermore, there is a lack of an audit trail across all of the Council's cyber traffic. There is a high risk associated with the current solution not protecting the organisation, and the corporate COVID 19 risk register highlights an increased risk of a successful phishing scam or cyber-attack. This decision will enable the Council to manage these risks more effectively.
Environmental Implications:	There are no environmental considerations to be taken into account
Legal Implications:	As detailed within this report an exemption to the Council's Contract Standing Orders will be required. The recommendation also includes a requirement in respect of any subsequent legal agreements.
Equality and Diversity:	There are no equality considerations to be considered in relation to this report. Therefore, an Equality Impact Assessment is not necessary.

Options:	As detailed within the report.
Recommendation:	As detailed within the report.
Reasons for Recommendation:	As detailed within the conclusion and the emergency decision section of the report.

Agenda No

Emergency Report - 15 June 2020

Proposal for a new all in one Web and Email security platform

Please select Report of the Head of Communities and Homes

Recommendation

1. The allocated budget of £0,060m for the implementation of a new all in one Web and Email security platform.
2. Approval of the award of contract to the proposed recommended system of Censornet as detailed within this report.
3. Delegated Authority to the Head of Communities and Homes in consultation with the Monitoring Officer to enter into all legal agreements with arising from the recommendation

1. PURPOSE OF REPORT

The purpose of this report is to propose the purchase and implementation of a new all in one Web and Email security platform.

2. BACKGROUND

The challenge of protecting confidential information has increased in recent years as more stringent data privacy regulation has been put in place through the GDPR, while at the same time digital transformation increases the volume and vulnerability of data. Visibility of where data is stored, and control over who has access to it and has the ability to share it is vital in this day and age.

With Rugby already well on the way in its digital transformation journey, having migrated to Microsoft Azure and Office 365, the IT department has identified that the organisation needs an additional layer of security on top of what was provided as standard by its cloud services. Unfortunately, during the COVID-19 crisis it became clear that current security suppliers do not have the necessary cloud security expertise or share RBC's ambition to modernise its digital estate and become more cost effective. It has become very clear that the legacy security products we are using are, ineffective and hard to maintain. They are no longer able to keep pace with how our environment has changed over the past few months, namely their ability to support a mobile workforce, and therefore are not fit for purpose.

One of the high-risk areas is the inability to identify and report on our email and web usage and the visibility and control of threats targeting the organisation originating from these sources.

The lack of an audit trail across all of our cyber traffic is another identified gap that needs filling. Additionally, we currently do not have a Cloud Access Security Broker (CASB).

CASB is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. A CASB acts as a gatekeeper, allowing the organization to extend the reach of their security policies beyond their own infrastructure.

CASB typically offers the following:

- Firewalls to identify malware and prevent it from entering the enterprise network.
- Authentication to checks users' credentials and ensure they only access appropriate company resources.
- Web application firewalls (WAFs) to thwart malware designed to breach security at the application level, rather than at the network level.
- Data loss prevention (DLP) to ensure that users cannot transmit sensitive information outside of the corporation.

How CASB works

CASB works by ensuring that network traffic between on-premises devices and the cloud provider complies with the organization's security policies. The value of cloud access security brokers stems from their ability to give insight into cloud application use across cloud platforms and identity unsanctioned use. This is especially important in regulated industries.

CASB uses auto-discovery to identify cloud applications in use and identify high-risk applications, high-risk users, and other key risk factors. Cloud access brokers may enforce a number of different security access controls, including encryption and device profiling. They may also provide other services such as credential mapping when single sign-on is not available.

3. PROPOSAL

3 options have been reviewed for their suitability for providing an all in one cyber security solution for Rugby Borough Council based on its ability to work with our current infrastructure and application base.

3.1 Option 1 – Censornet

The Censornet platform provides a single pane of glass view across multiple critical solutions, simplifying security, architected specifically for organisations.

The Censornet platform enables organizations to move away from the more expensive approach of running separate solutions in silos and allows security teams to manage security defences core effectively and efficiently, in a way that reflects how modern enterprises work today. The Censornet platform allows users the freedom to access the applications and data they need - regardless of device or location, whilst providing visibility for IT and protection for all.

Dashboards and Reporting – the Censornet platform provides rich data visualization and reporting across all Censornet services and an extensive set of attributes and criteria. Each administrator has their own Home Dashboard with charts and widgets specific to the services licensed. Multiple standard reports are included for each service within the Analytics section of the portal. Detailed analysis and reporting is available by time, user, device (hostname and MAC address), URL category, web category, cloud application class, cloud app name, cloud app action, keyword (e.g. filename, comment, login details), policy name, risk level, email direction, delivery status (delivered, spam, virus), outcome (block or allow).

The Censornet platform consists of:

- Email – secure your entire organization from known, unknown and emerging email security threats including email fraud.
- Web – protect users from web borne malware, offensive or inappropriate content and improve productivity
- CASB – discover, analyse, secure and manage user interaction with cloud applications - inline and using APIs.

3.2 Option 2 – Mimecast

Mimecast's cloud-based Secure Email Gateway protects organisations and employees using any cloud or on-premises email platform. It defends against inbound spear-phishing, malware, spam and zero-day attacks by combining innovative applications and policies with multiple detection engines and intelligence feeds.

Your information, and ultimately your business' reputation, is protected by outbound scanning of all emails to block threats and prevent malicious or unintentional loss of sensitive or confidential information.

Mimecast Web Security protects against malicious web activity, blocks business-inappropriate websites and helps mitigate shadow IT risks caused by uncontrolled cloud app use. Easy to deploy and manage, it gives you the technology needed to keep the web safe, delivered in the most cost-effective and least complex way possible.

3.3 Option 3 – Barracuda

The Barracuda platform consists of:

- Option 3 – total email protection bundle combines Essentials, Sentinel, PhishLine and Forensics and Incident Response
- Essentials all-in-one email security, backup and archiving service
- AI-based protection from spear phishing, account takeover and business email compromise
- PhishLine anti-phishing training and simulation platform
- Forensics and Incident Response automated incident response and threat insights
- Archiving solutions for data retention, compliance and e-discovery

4. FINANCIAL INFORMATION

4.1 Option 1 – Censornet

Capital cost – one upfront payment of £0.060m

Users	Product	Year 1	Year 2	Year 3	Year 4 onwards
		2020/21 £000s	2021/22 £000s	2022/23 £000s	2023/24 £000s
600	Censornet E Mail Security	20	0	0	7
600	Censornet Web Security	16	0	0	5
600	Censornet CASB	24	0	0	8
		60	**-**	**-**	**20**

After the three years, an annual subscription will be required. This will be an annual charge of £0.020m and it is anticipated that this will be funded from existing budgets within the team

Capital cost – if we choose to pay annually £0.022m

Users	Product	Year 1	Year 2	Year 3	Year 4 onwards
		2020/21 £000s	2021/22 £000s	2022/23 £000s	2023/24 £000s
600	Censornet E Mail Security	7	7	7	7
600	Censornet Web Security	6	6	6	6
600	Censornet CASB	9	9	9	9
		22	**22**	**22**	**22**

The recommendation would be to fund this system through Capital as a one-off payment in 2020/21. This option would result in a revenue saving of £8,000 for years 1 – 3, as the budget for the current system will no longer be needed.

4.2 Option 2 – MimeCast

This option is the most expensive and given that it does not meet all our functional needs it is not really a realistic option. The organisation has quoted £0.050m as the annual fee, so over a three-year contract the total cost would be in the region of £0.150m.

Quantity	Product	Year 1	Year 2	Year 3
		2020/21 £000s	**2021/22 £000s**	**2022/23 £000s**
600	Mimecast M3RA - Licence	30	30	30
600	Mimecast Add on - Large File Send - Licence	4	4	4
600	Mimecast W1 - Licence	9	9	9
1	Mimecast LCS - Gold - 1 Year - Licence	4	4	4
1	Mimecast Web Security Implementation - Licence	3	3	3
		50	**50**	**50**

4.3 Option 3 – Barracuda

Email and Web Barracuda – three years

Barracuda is mid-range cost but as with Mimecast does not provide all the required functionality that we need to protect our environment as well as we would like.

Quantity	Product	Year 1	Year 2	Year 3
		2020/21 £000s	**2021/22 £000s**	**2022/23 £000s**
600	Barracuda Total Email Protection - EDU 3yrs	13	13	13
600	Barracuda Content Shield Entry Subscription 3yrs	5	5	5
600	Barracuda Content Protection Subscription 3yr	3	3	3
600	Barracuda Web Content Agent Subscription 3yrs	3	3	3
		24	**24**	**24**

5. CONCLUSIONS

A proof of concept is currently underway with the Censornet solution which is due to finish on 4 June 2020 and it has up until now provided all the functionality we require. The all in one solution will give us better protection against threats than we have with our current solutions and much improved reporting functionality which external auditing has identified as a current weakness.

The recommended system, Censornet, would cost a one-off £0.060m which provides the organisation with 3 years of an improved cyber security system with better functionality and an integrated all in one solution. This will give the organisation peace of mind over email and web security, particularly in the audit and reporting modules.

Potentially, there could be high-risk associated with the current solution not protecting the organisation.

The importance of this solution and the increased protection and reporting capabilities it will provide.

It is recommended that this proposal is actioned. Due to the urgency of this decision an exemption request of the required constitutional contract standing orders is in the process of being considered and is expected to be approved.

6. Emergency Decision

This decision is being made under emergency constitutional powers. This is due to COVID-19 and the inability for the Council to hold Full Council meetings. The Council has now held its first virtual Cabinet meeting but presently is undertaking work in preparation for the first Full Council meeting on the 21st July. In the absence of such meetings there are emergency powers that can be exercised by the Executive Director. This is in consultation with Group Leaders, the Mayor and the Chairman of Overview & Scrutiny.

An urgent decision is required to fully protect the Council and have the required IT infrastructure in order for this to be achieved. This has arisen directly through the demand on IT services as a result of COVID-19.

If the Council is not able to progress this by the end of June, then this will result in potential risks to the Council and subsequently potential significant disruption to the Council. This means that an emergency decision is required as set out within the Council Constitution and the Council cannot await the presently scheduled Full Council meeting of the 21st July.

Name of Meeting: Emergency Report

Date of Meeting: 15 June 2020

Subject Matter: Proposal for a new all in one Web and Email security platform

Originating Department: Communities and Homes

DO ANY BACKGROUND PAPERS APPLY ☐ **YES** ☒ **NO**

LIST OF BACKGROUND PAPERS

Doc No	Title of Document and Hyperlink

The background papers relating to reports on planning applications and which are open to public inspection under Section 100D of the Local Government Act 1972, consist of the planning applications, referred to in the reports, and all written responses to consultations made by the Local Planning Authority, in connection with those applications.

☐ Exempt information is contained in the following documents:

Doc No	Relevant Paragraph of Schedule 12A