

For Publication

Bedfordshire Fire and Rescue Authority
Audit and Standards Committee
21 Sept 2021

REPORT AUTHOR: PAUL HUGHES
SUBJECT: CYBER SECURITY UPDATE

For further information on this report contact: Graham Fox
Infrastructure Manager, ICT Shared Service
Tel No: 01234 413215

Background Papers: N/A

Implications (tick ✓):

LEGAL			FINANCIAL	
HUMAN RESOURCES			EQUALITY IMPACT	
ENVIRONMENTAL			POLICY	
CORPORATE RISK	Known	✓	OTHER (please specify)	
	New			

Any implications affecting this report are noted at the end of the report.

PURPOSE:

To provide The Audit and Standards Committee with a Cyber Security update.

RECOMMENDATION:

That Members acknowledge progress to date

1. Cyber Security Update

- 1.1 The Cyber Security threat landscape is constantly evolving, and comprehensive security measures are updated and reviewed regularly.
- 1.2 BFRS utilises many security defence mechanisms, encompassing people, process and technology.
- 1.3 BFRS has gained re-accreditation of the National Cyber Security Centre (NCSC) security standard - Cyber Essentials Plus in August 2021 and Basic Cyber Essentials May 2021. This follows original accreditation for the Basic Cyber Essentials standard in 2019, followed by Cyber Essentials Plus in 2020. Cyber Essentials Plus accreditation will be an annual accreditation exercise using recognised 3rd parties to take BFRS through the independent assessment process.
- 1.4 BFRS has previously utilised RSM to have a targeted security audit to enable the successful accreditation of Cyber Essentials in 2019 and 2020.
- 1.5 Cyber Security Awareness Training is being set up on the BFRS LearnPro system. This will be mandatory training for all staff. This will be available in Autumn 2021. This is a Security Awareness course provided by NCSC.
- 1.6 ACO Chambers continues to Chair the quarterly Information Management Assurance Board (IMAB) which is a joint board with Bedfordshire Police whom provide our Data Protection Officer (DPO) service with the DPO a stakeholder on the IMAB board.

- 1.7 BFRS and Cambridgeshire FRS has jointly commissioned a 3rd party to perform a Cyber Security Review. The outcome is a Recommendations and Gap analysis report. This will support an overarching cyber strategy / roadmap for a multi layered approach for reactive and proactive measures including Cyber KPI's.
- 1.8 Cyber Security is a standing agenda item at the quarterly NFCC ICT Managers forum, which HICT attends.
- 1.9 ICT Shared Service has a monthly Cyber Security meeting, chaired by the ICT Infrastructure Manager. This enables progress updates against set BAU security tasks, patch management actions etc. as well as horizon scanning for future threats.
- 1.10 The annual Network Penetration Test (PEN) test is scheduled for November 2021. There are typically remediations from this which are tracked through the ICT Monthly security meeting.
- 1.11 BLRF – Cyber Working Group established in June 2021 represented by Rich Gordon – Group Commander Response. The aim of the group is to help deliver National Resilience Standards for LRFs – Standard #14 “Cyber Incident Preparedness”.
- 1.12 There is a Cyber Security item on the Corporate Risk Register to ensure appropriate governance and dialogue.
- 1.13 BFRS is reviewing its insurance to ascertain costs for Cyber Security insurance.

2. **Summary**

- 2.1 These are the main highlights and areas of work which demonstrate a wide portfolio of activities which support the BFRS Cyber Security needs.

3. **Graphic depicting BFRS cyber threats encountered during August 2021**

Figure 1 Mimecast Security Summary for August 2021



Key items to note from figure 1 is that BFRS received 134,677 emails in August. 12% of these emails were rejected, which in numbers is just over 16,000 emails. The graphic also shows 233 emails blocked for impersonation attempts (phishing) and 12,203 email attachments sandboxed i.e. further security checks performed.

PAUL HUGHES
HEAD OF ICT AND PROGRAMMES