Standards and Governance Committee

Purpose: Noted

Date: **31 January 2019**

Title: **INFORMATION SECURITY UPDATE**

Report of Chief Fire Officer

SUMMARY

1. The purpose of this report is to provide the Standards and Governance Committee with an update on the cyber-attack suffered by Hampshire Fire and Rescue Service (HFRS) on 21 August 2018.

2. This report also provides awareness of the new requirement under General Data Protection Regulations (GDPR) for Hampshire Fire and Rescue Service (HFRS) to report data breaches to the Information Commissioner's Office (ICO) that have been assessed as presenting a risk to individuals within 72 hours of HFRS becoming aware that the incident has taken place.

3. This report is to provide the Standards and Governance Committee of Hampshire Fire and Rescue Authority (HFRA) with assurance of the measures taken and that HFRS is managing any personal data breaches in compliance with data protection legislation.

BACKGROUND

4. Since 25 May 2018 there is a new requirement for public bodies under the GDPR to report, within 72 hours, any personal data breaches assessed as presenting a risk to individuals to the ICO.

5. The HFRS Governance and Compliance team will assess the level of risk associated with a breach in the light of the legislation and ICO guidance to determine whether an incident is reportable to the ICO.

6. As a result of this requirement there is a potential for an increase of reportable data breaches to the ICO. This is not indicative of more personal data breaches occurring but increased transparency due to the new requirement of reporting data breaches where required. Reporting personal data breaches that present a risk to individuals to the ICO is in compliance with the GDPR and Data Protection Act 2018.

7. If HFRS were to not report relevant data breaches to the ICO, the Service would be in contravention of the GDPR and Data Protection Act 2018.

DATA BREACH

8. A total of 21 HFRS employee accounts were accessed by an unknown party without authorisation in the Summer of 2018.

9. Of these 21 HFRS accounts, 30 documents were opened of which 6 contained some personal data.

10. This incident is believed to have been caused by phishing emails received by staff. The body of the emails referred to outstanding invoices, needing assistance to review documentation etc. They generally included an attachment which users were encouraged to open.

11. HFRS has not received any complaints in connection with this incident.

12. On the 24 August 2018 this data breach was reported to the ICO.

REMEDIAL ACTION

13. The cause of this data breach has been identified as a series of IT security failures including a lack of cyber security resource within HFRS, lack of and poorly performing security software solutions and security measures, such as simple passwords.

14. Action was taken immediately to shut down access to HFRS systems, force password changes on all accounts and implement enhanced security software to stop any further compromise of accounts and identify any malicious software within the HFRS network.

15. With the incident locked down, further tasks were undertaken to review and plan higher security standards and solutions that have been or are now being implemented.

SUPPORTING OUR SERVICE PLAN AND PRIORITIES

16. HFRS is committed to making Hampshire safer. HFRS takes the responsibility bestowed on us to process personal information very seriously and has made monitoring compliance with data protection legislation one of our priorities.

RESOURCE IMPLICATIONS

17. The Hampshire Fire and Rescue Authority (HFRA) approved in December 2018 to increase cyber security expertise within the ICT department.

18. HFRA also approved through the Medium Term Financial Plan, financial resources to implement improved IT security measures including those outlined within this report.

ENVIRONMENTAL AND SUSTAINABILITY IMPACT ASSESSMENT

19. There is no environmental and sustainability impact.

LEGAL IMPLICATIONS

20. The ICO can take regulatory action and fine HFRS up to £17M and affected individuals can take legal action against HFRS if we are found to be non-compliant with data protection legislation.

EQUALITY IMPACT ASSESSMENT

21. Compliance with Data Protection legislation is essential for HFRS to protect the human rights of our employees and members of the public.

OPTIONS

22. This report asks the Authority to note the information. This report provides the Authority with assurance that the Service is adhering to ICO requirements.

23. This report provides the Authority with relevant information to scrutinise the Service and the commitments it has made in relation to compliance with data protection legislation.

RISK ANALYSIS

24. HFRS operates a robust procedure for the investigation of personal data breaches. We are transparent with the ICO and data subjects (the individuals the information is about) regarding our compliance with data protection legislation. If HFRS were to not report personal data which present a risk to individuals to the ICO, the Service would be in contravention of the GDPR and Data Protection Act 2018.

CONCLUSION

25. The root cause of the breach has been identified and actions have been put in place to prevent a reoccurrence of a similar incident.

26. This report is to provide the Authority with assurance that HFRS is managing any personal data breaches in compliance with data protection legislation, including the new requirement under GDPR for HFRS to report

relevant data breaches to the ICO within 72 hours of the Service being made aware of them.

RECOMMENDATION

27. That this report be noted by Hampshire Fire and Rescue Authority Standards and Governance Committee.

Contact: Matt Robertson, Chief of Staff, matt.robertson@hantsfire.gov.uk
07918887532