FREEDOM OF INFORMATION RESPONSE

Ref: FOI 269

Response date: 7th May 2025

You asked Money and Pensions Service the following

1. Details of any/all cyber security incidents within the last 5 years.
2. Details of any/all qualifications held by employed parties directly involved in cyber security provisions.
3. Details of any contracts maintained by the Money and Pensions Service, in relation to cyber security provisions.
4. Details of direct spend in relation to cyber security.
5. Details of strategic KPIs/KRIs that impact cyber security.

Money and Pensions Service Response

We are treating your correspondence as a request for information under the Freedom of Information Act 2000. We confirm that we hold the information. The information we can provide is as follows:

1. The only cyber-attacks of relevance have been a small number of DDoS attacks against the main website.
2. ISO27001, CyberEssentials Plus, SOC2.
3. Please see below.
4. Spend is in the region of £300k per annum.
5. All strategic KPIs/KRIs are impacted by cyber as cyber has an overarching element to all organisations.

In relation to Question 3, we can only answer in part. MaPS has a number of security contracts with external

providers such as Security Operation Centre (SOC), pen testing and managed services. However, disclosure of the contract details would be likely to unfairly prejudice MaPS. As a consequence, the information requested is exempt from disclosure under section 30(1)(a) of FOIA.

"Section 31(1)(a) of FOIA states that: "Information …. is exempt information if its disclosure under this Act would, or would be likely to, prejudice- (a) the prevention or detection of crime,".

MaPS like any organisation may be subject to cyber-attacks and, since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important. The release of contractual information would likely enable cyber-attacks and thus prejudice the prevention and detection of crime. Cyber-attacks may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998. We

consider that there are a number of different areas where the risk of crime would be likely to increase such as fraud / scamming of MaPS customers and partners.

In addition, publishing the requested information would provide information about MaPS information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing MaPS information systems from being subject to cyber-attacks. Providing the type of information requested would be likely to provide attackers with information relating to the state of our cyber security defences, and this is not in the public interest.

We consider that the release of this information into the public domain would enable attackers to identify and therefore target MaPS. When considering the public interest in detecting and preventing crime, it is important to take account of the consequences that can reasonably be anticipated and which we have already identified.