DORSET & WILTSHIRE FIRE AND RESCUE

Freedom of Information Request FOI 18 17

Cyber Security

Query:

As a Freedom of Information request, please supply the following information.

1. Does your organisation adhere to the Network Security guidance outlined by the National Cyber Security Centre, within its '10 Steps to Cyber Security'?

    - Yes
    - No

2. Do you ensure that security patches for critical vulnerabilities are routinely patched within 14 days, as recommended by the National Cyber Security Centre?

    - Yes
    - No

3. Have you suffered from any service outages on your network in the last two years, however small?

    - Yes
    - No

4. Did any of these outages cause a loss, reduction or impairment to your organisation's delivery of essential services?

    - Yes
    - No

5. Was the root cause of the service outage identified and confirmed – at the time or afterwards?

    - Yes
    - No

6. Is it possible that any service outages you have suffered in the last two years was caused by a cyber-attack – such as ransomware, DDoS attack, or malware?

    - Yes
    - No

7. Are you aware that Distributed Denial of Service (DDoS) attacks are a significant contribution to service interruptions, outages and downtime?

    - Yes
    - No

Response

1. Does your organisation adhere to the Network Security guidance outlined by the National Cyber Security Centre, within its '10 Steps to Cyber Security'?

    - Yes

We confirm that we hold some of the information that you have requested. However, the information requested in questions 2-6 is withheld under Section 24 (National Security) and Section 31 (Law Enforcement).

Section 24

Section 24 exempts information for the purpose of safeguarding national security. It is a qualified exemption, which means that it is subject to a public interest test.

We acknowledge the public interest in openness and transparency, but we consider that there is also a public interest in DWFRS protecting national security. Disclosure of information about our cyber security measures could allow individuals to assess the strength of our defences and undermine the confidentiality and integrity of our systems. Consequently, this could then have an adverse impact on the UK's security. We have therefore concluded that this exemption applies and that non-disclosure serves the public interest better than release in this instance.

For these reasons, we consider that the public interest in maintaining this exemption outweighs the public interest in disclosure.

Section 31

The exemption in section 31(1) (a) is designed to cover all aspects of the prevention and detection of crime.

Section 31 is a qualified exemption, which means that it is subject to a public interest test. We acknowledge the public interest in openness and transparency and we recognise that releasing this information would provide the public with assurance that we are appropriately protecting our ICT systems. However, disclosure of the information requested could aid a criminal who was intent on launching an attack on our ICT systems and could expose DWFRS to potential threats, such as targeted e-crime and threats of a criminal nature. DWFRS takes protection of its ICT infrastructure very seriously.

For the reasons set out above, we have assessed that the public interest in maintaining this exemption outweighs the public interest in disclosure.

7 Are you aware that Distributed Denial of Service (DDoS) attacks are a significant contribution to service interruptions, outages and downtime?

    - Yes