Mae'r ddogfen yma ar gael yn Gymraeg

Agenda Item 10

Report to	**Executive Panel**
Date	**12 December 2022**
Lead Officer	**Richard Fairhead, Assistant Chief Fire Officer**
Contact Officer	**Steve Morris, ICT Technical Manager**
Subject	**Cyber Essentials (CE) Certification**

PURPOSE OF REPORT

1. To inform members of the North Wales Fire and Rescue Authority (the Authority) of the work the service is undertaking with regards to cyber security.

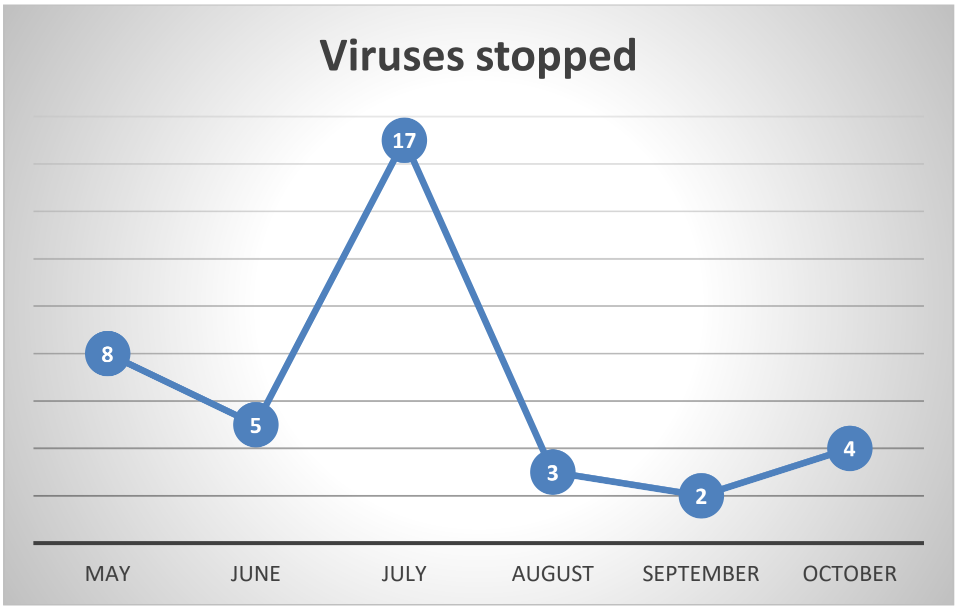
RECOMMENDATION

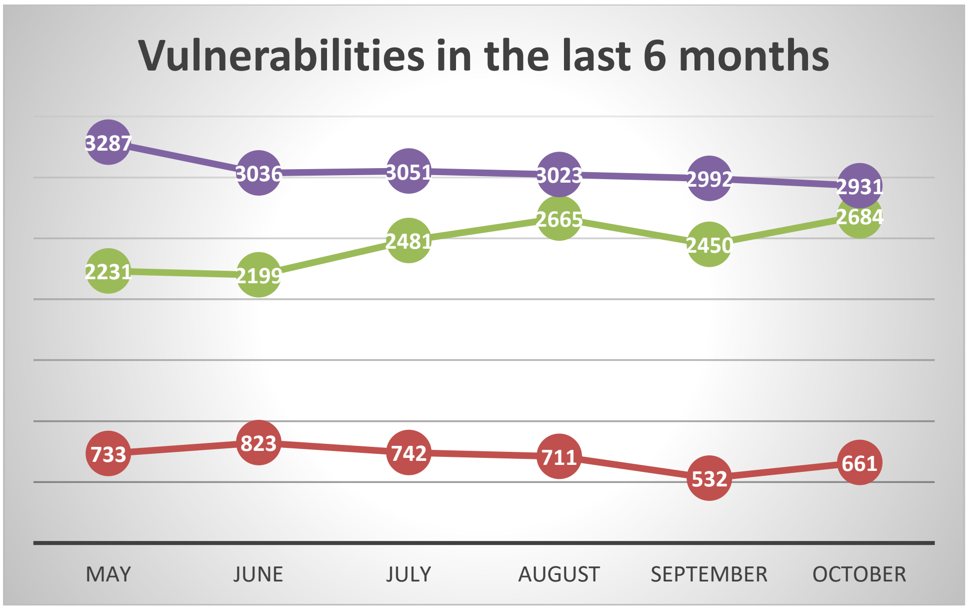
2. Members are asked to:
   i) Note the work being carried out by the Service on cyber protection, including the Service working towards CE certification in the first instance.

INFORMATION

3. All organisations are under constant threat from cyber criminals trying to attack computer systems and North Wales Fire and Rescue Service (the Service) is no different. Our ICT department are, on a daily basis, identifying and stopping these attacks and preventing threats entering our systems. This work is continuous and a significant amount of time and resources are spent protecting the service from cyber-attack.

4. The graphs on page 2 of this report show the extent of the work required by the ICT department to protect us from cyber threats. In the last 6 months our ICT department has identified and dealt with 39 viruses' trying to enter and over 6,000 threats have been identified which our systems have to deal with and prevent entering our systems. The Service's Firewalls, which are programmes that monitor what is coming in and going out of our systems and block threats, are constantly being updated to ensure they are effective.





Critical Risk	High Risk	Medium Risk

5. If we didn't work so hard to identify viruses and threats then there are several different ways in which the Service would be affected.

    a. If a cyber-criminal accessed our risk critical command and control systems, we may not be able to mobilise fire engines.
    b. If personal data was accessed and then leaked we would be liable to a fine of up to 20 million euros.
    c. Cyber criminals try to disable organisations systems using ransomware which require both time and considerable cost to re-instate.
    d. Falling victim to cyber criminals would also cause reputational damage the service.

6. The National Cyber Security Centre have an initiative called Cyber Essentials (CE) that is designed to assist organisations against the ever-growing threat of cyber-attacks. As such, Welsh Government (WG) are encouraging all public sectors to meet the CE standard, which is a self-assessment addressing how to prevent the majority of cyber-attacks, whilst working towards Cyber Essentials Plus (CE+) which is a more in-depth assessment carried out by an independent assessor.

7. The Service are currently working to achieve CE certification in the first instance, and following the self-assessment will work towards preparing for the independant assessment to achieve CE+. Achieving CE+ will require investment in technology and staff who have the skills to work full time on addressing the cyber security issues.

8. Colleagues at the other two Welsh Fire and Rescue Services (FRS) are also looking to achieve CE before working towards CE+ certification due to similar resourcing challenges. Other public sector organisations such as North Wales Police (NWP) have achieved certifications similar to CE+. However, they have invested the resources to achieve this due to the nature of their business and sensitivity of the data they hold.

9. The ICT department will continue to invest significant time and resources to protecting the Service but having a certification such as Cyber Essentials offers independent assurance that serious measures have been taken to protect our computer systems. It also provides the Service with a clearer picture of any potential areas where improvement may be required.

IMPLICATIONS

Well-being Objectives	N/A
Budget	CE is £700 per annum CE+ is £2700 per annum. Significant investment for both staff and technology is also required.
Legal	Not applicable, although the Service could face legal consequences should a cyber-attack hamper its ability to carry out its statutory duties.
Staffing	Meeting the standards that would allow CE+ accreditation would require a skilled technical resource dedicated to the cyber security fight. This resource is not a resource we currently have
Equalities/Human Rights/Welsh Language	N/A
Risks	The risks of not being cyber secure are far reaching and can include: an inability to function as a Service; large financial costs and time involved in recovery; reputational damage; and legal complications.