Portfolio Holder Report

The portfolio holder will make a decision on this item after seven days have elapsed (including the date of publication).

Report of:	Portfolio Holder	Date of publication
Clare James, Corporate Director Resources (and S151 Officer)	Cllr Michael Vincent, Resources Portfolio Holder	22 March 2022

ICT Cyber Resilience and Disaster Recovery Measures

1. Purpose of report

1.1 To approve the procurement of Vulnerability Scanning Software to reduce the opportunity for successful cyber-attacks through ensuring all vulnerabilities are identified and patched at the earliest opportunity.

2. Outcomes

2.1 To ensure better protection for council ICT systems from future cyber-attacks.

2.2 To enable the council's ICT service to effectively identify internal and external issues in applications and operating systems and ensure all vulnerabilities in council systems are addressed at the earliest opportunity.

3. Recommendation

3.1 That the council enters into a contract with Tenable Ltd for the provision of their Vulnerability Scanning and Reporting System.

4. Background

4.1 The Digital Revolution is changing the world. The pace of change driven by technology over the past 10 years has been breath-taking and will only continue to increase at a faster rate in the future.

4.2 The reliance on technology is only going to increase in the future, as just like every other private and public sector organisation, the council is busy "going digital". This can be defined as "the process of adopting digital technologies to help improve and streamline the business, while at the same time giving customers' access to services at a time and in a way

that suits them". By default, this process introduces more technology and systems for the council's ICT provision to manage and support.

4.3 While the increasing use of digital services and technology brings many benefits to the council, it also increases the ever growing possibility of being the victim of a cyber-attack. Each time we add new systems, services and applications, we increase our footprint in the digital world and increase the chances of an attacker finding a vulnerability and being successful in executing an attack. The government recently wrote to all local authorities warning of an increased threat of cyber-attacks on public bodies as a result of the conflict in the Ukraine.

5. Key issues and proposals

5.1 Cyber-attacks on public sector software systems are becoming increasingly common and in most cases the cost of recovery from such attacks has proved to be significant for the organisation.

5.2 A Ransomware attack on the ICT systems in use at Redcar and Cleveland Council in February 2020 left them having to resort to using pen and paper for weeks while they tried to recover their systems. In the weeks following the attack the council website and telephony systems could not be used. The cost of re-instatement associated with the cyber-attack at Redcar and Cleveland was reported to be in excess of £10 million for which the government only partially compensated the council.

5.3 More recently, a cyber-attack carried out on 20 December 2021, by what is believed to have been a group of Russian hackers, left Gloucester City Council unable to operate its revenues, benefits and planning services, until it had rebuilt the associated software systems and the servers they were sat upon. This was the second such attack against Gloucester City Council in a decade.

5.4 The threat of a cyber-attack on Wyre Council ICT systems is very real, indeed such an attack was attempted in December 2021. However, on that occasion the security systems already in place successfully repelled the attack.

5.5 The ongoing conflict in Ukraine has already shown many times over just how damaging cyber-attacks can be to organisations and the Government have very recently seen fit to issue a warning to all public sector bodies in the UK advising them of an increased threat of a cyber-attack on public sector ICT systems as a consequence of the conflict.

5.6 At present our ability to identify the vulnerabilities in council systems is limited to our annual PSN health check. This identifies existing vulnerabilities on a percentage of council systems at a point in time. On average it highlights at least 150 medium to critical vulnerabilities every year, which we then resolve over the course of the following 12 months. Therefore we are at risk for a period of time before we can patch the vulnerabilities, leaving us at greater risk of an attack.

5.7 A limited number of external organisations provide software or services that enable public sector organisations to better protect themselves from cyber-attacks. However, as there are a limited number, the costs associated with most of these solutions are prohibitive. After careful research into the most appropriate solution that will assist Wyre to better protect itself from attack, at a reasonable cost, the solution provided by Tenable Ltd is considered to be the best option.

5.8 Tenable Ltd offer a vulnerability scanning solution that will allow us to carry out as regularly as we choose, the same checks on our entire infrastructure that are carried out in our annual PSN health check. This will allow for the rectification of any issues identified on a monthly, weekly or even daily basis. It provides details for remediation of all vulnerabilities found and the ability to retest specific vulnerabilities after patching has been completed.

5.9 The Tenable solution also provides an extensive reporting module, meaning we can keep an accurate track of remediation progress and will have a visible means of representing our vulnerability/threat posture. It will also allow us to produce management reports to ensure that we have the relevant records on the risk register and to provide reassurance that we are effectively reducing our vulnerability footprint and that the product is being used to its full potential.

5.10 The vulnerability scanning software from Tenable Ltd costs £39,018 over three years. The costs will be met from general balances as they represent a new and ongoing budget requirement.

5.11 This is the latest stage in strengthening our cyber resilience measures and a further report will be issued in due course regarding the provision of back-up software systems should a cyber-attack on council ICT systems be successful.

6. Delegated functions

6.1 The matters referred to in this report are considered under the following executive function delegated to the Resources Portfolio Holder (as set out in Part 3 of the council's constitution): "To consider progress on the implementation of the Council's ICT digital strategy."

Financial and legal implications	
Finance	The cost of the Tenable solution is £39,018 over three years (£13,006 per annum). The cost represents an additional ongoing requirement for which no base budget exists. As such the cost will be met from general balances and the Medium Term Financial Plan will be updated to reflect this.

Legal	A contract will be entered into with Tenable Ltd for the provision of their Vulnerability Scanning and Reporting System.

Other risks/implications: checklist

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report, for those issues marked with a x.

risks/implications	**✓ / x**
community safety	x
equality and diversity	x
sustainability	x
health and safety	x

risks/implications	**✓ / x**
asset management	x
climate change	x
ICT	✓
data protection	✓

Processing Personal Data

In addition to considering data protection along with the other risks/ implications, the report author will need to decide if a 'privacy impact assessment (PIA)' is also required. If the decision(s) recommended in this report will result in the collection and processing of personal data for the first time (i.e. purchase of a new system, a new working arrangement with a third party) a PIA will need to have been completed and signed off by Data Protection Officer before the decision is taken in compliance with the Data Protection Act 2018.

report author	telephone no.	email	date
Peter Mason	01253 887530	Peter.mason@wyre.gov.uk	21 March 2022

List of background papers:		
name of document	date	where available for inspection
None		

List of appendices
None