ADUR & WORTHING
COUNCILS

Joint Governance Committee
25 September 2018
Agenda Item 9

Ward(s) Affected: n/a

Value/Cost of more frequent network penetration testing

Report by the Director for Digital & Resources

Executive Summary

1. Purpose

1.1. This reports addresses cyber security associated with the Councils IT systems and data; exploring the value of increasing proactive testing (known as penetration testing) to identify and close vulnerabilities.

1.2. The Councils have security processes in place that include regular system security updates and independent security testing, which is a requirement of the Cabinet Office for access to the Public Services Network (PSN). However, the Councils now operate some services through cloud providers and the strategy is to operate more services from the cloud. The scope of the current security testing does not include cloud services.

1.3. Security testing is currently carried out once annually as part of the PSN compliance requirement. Given the need to include cloud services under the scope of security testing, the ongoing risk of cyber attacks, and the potential financial implications of a data breach under GDPR, there is a need to review the frequency of security testing to ensure any vulnerabilities are surfaced quickly and closed.

1.4. This report sets intentions to change to the frequency and scope security testing to provide greater assurance that systems, services, and data have the best available protection against cyber attacks.

2. Recommendation

2.1. The Committee is asked to note the content of this report.

3. Context

3.1. Currently, in addition to the Council's own system security updates, independent security testing is carried out annually with focus on services that reside at the Town Hall. This annual test, its findings, and remediation plans are a requirement of the Cabinet Office for access to the Public Services Network (PSN) and therefore must continue.

3.2. The current cloud service providers test their services rigorously to ensure they are secure and not subject to vulnerabilities. However, the current 'independent' tests commissioned by the Councils do not include these cloud services and there should be the independent verification that external services are and remain to be secure. Furthermore, the current test, carried out once annually, produces a high-workload for remediation putting pressure resources and leaving vulnerabilities open for longer than necessary.

3.3. The Councils will extend the scope of independent security testing. The change of scope to include cloud services will provide assurance that the infrastructure's that are beyond the control of the Councils are adequately protected, and the increase in testing frequency will ensure vulnerabilities that arise surfaced and closed more promptly.

4. Issues for consideration

4.1. The issue that has been reviewed to form this paper surrounds the scope and frequency of independent security testing, which is currently carried out once per annum. The current scope will not adequately cover all services in future i.e. the cloud providers independently test their environments, but there is a need for the Councils to have independent verification on the level of protection in place for its cloud services.

4.2. Furthermore, the 'once per annum' frequency of testing leaves too greater period between tests. To address these issues Councils will

extend the scope to include cloud services and scheduling quarterly 'mini' tests throughout the year.

5. Engagement and Communication

5.1. This report has been developed through engagement with the Councils' Digital / IT Team.

5.2. Further engagement with the Councils' security partners will take place to identify costs and options for achieving greater assurance that all systems and services are protected and maintained.

6. Financial Implications

6.1. The delivery of increased penetration tests and the expansion of scope of the testing regime cannot be accommodated within existing budgets. At present the options for a new testing regime and the associated pricing are being identified.

6.2. Once the cost has been quantified, a growth bid will be submitted as part of the 2019/20 budget round which members will consider alongside other such bids.

7. Legal Implications

7.1. Section 1 of the Localism Act 2011 provides the Council with the power of general competence to do anything that an individual may do.

7.2. Section 111 Local Government Act 1972 allows a local Authority to do anything which is calculated to facilitate or is conducive or incidental to the discharge of any of their functions.

Background Papers

- DR Test & Beyond

Officer Contact Details:-
Name: Robert Wood
Role: IT & Digital Services Manager
Telephone: 07736 597499
Email: robert.wood@adur-worthing.gov.uk

Sustainability & Risk Assessment

1. Economic

- Matter considered and no issues identified.

2. Social

2.1 Social Value

- Matter considered and no issues identified.

2.2 Equality Issues

- Matter considered and no issues identified.

2.3 Community Safety Issues (Section 17)

- Matter considered and no issues identified.

2.4 Human Rights Issues

- Matter considered and no issues identified.

3. Environmental

- Matter considered and no issues identified.

4. Governance

- The resilience of the Council's ICT and Digital Infrastructure is critical to our ability to deliver our services. The increase in security testing frequency and scope will provide greater assurance that systems are secured and available for Council staff and customers.

- The continued stability and accessibility of ICT services and Digital services enhances the reputation of the Councils.