Report to Audit Committee

21 September 2021
Director of Corporate Resources
INFORMATION REPORT

Not Exempt

Cyber Insurance Review and Cyber Security Awareness and Defences

Executive Summary

Review of the current Cyber Insurance market informs us that at this time, taking out Cyber Insurance would be costly and would likely result in duplication of cover on items such as fraud, equipment insurance and indemnity.

The Council should for now invest in improving our Cyber awareness and defences by training officers and members, as well as in areas such as Intrusion Detection, Multi Factor Authentication and Real time Monitoring.

This would also potentially reduce premiums if later, we decided to purchase Cyber Insurance. It is advisable to wait until the Cyber Insurance market has matured to try to prevent any duplication of cover.

Recommendations

Increase cyber defences and awareness using existing Technology Services budget. Revisit whether Cyber Insurance should be taken out as part of the annual budget cycle.

Background Papers

Cyber Insurance Analysis Report compiled by David Copland, IT Security Officer.

Cyber Insurance Analysis V3.1.docx

Wards affected: All Wards

Contact: Andrea Curson, Head of Customer and Digital Services 01403 215457.

Background Information

1 Introduction and Background

1.1 The Audit Committee raised the question of whether the Council should take out Cyber Insurance in light of a number of high-profile Cyber-attacks on public bodies and private companies. At this time the recommendation is not to do so but to concentrate efforts on improving Cyber awareness and defences.

1.2 The issue of Cyber Security is one that needs to be considered by the Council as the services it offers its residents may be adversely affected by a Cyber-attack.

1.3 The Council will focus on increasing Cyber awareness through training and defences to minimise risk of exposure, as oppose to taking out Cyber Insurance at this time due to market immaturity, cost, and duplication of cover with other insurance policies.

2 Relevant Council policy

2.1 This reports the Corporate Plan objective of a modern and flexible Council.

3 Details

3.1 To increase Cyber awareness through training for officers and members by sessions written and run by the Council's IT Security Officer.

3.2 We have a plan to improve our Cyber defences in line with National Cyber Security Council (NCSC) guidance, in the following areas. End Point protection to guard against ransomware attacks by the end of 2021, to investigate and procure real time monitoring of potential Cyber Security threats, to investigate options around Intrusion Protection and to continue rolling out Multi Factor Authentication to all.

3.3 The reason for choosing to increase Cyber awareness through training and to improve our Cyber defences as oppose to taking out Cyber Insurance is due to market immaturity, cost, and duplication of cover with other insurance policies.

4 Next Steps

4.1 The Council to continue to improve its Cyber awareness and improve its defences.

5 Views of the Policy Development Advisory Group and Outcome of Consultations

5.1 A review of the Cyber Insurance market was undertaken by Horsham District Council's Information Security Officer, Technical Accountant, the Head of Finance and Performance and Horsham District Council's Insurance Advisor. The full report is listed in the Background Papers section of this report.

5.2 The Director of Corporate Resources and the Monitoring Officer were consulted to ensure legal and financial probity.

5.3 There are no staffing issues.

6 Other Courses of Action Considered but Rejected

6.1 Taking out Cyber Insurance. This has been rejected due to market immaturity, cost and duplication of cover with other insurance policies.

7 Resource Consequences

7.1 There are no financial consequences arising from this report, as any expense for increasing our Cyber defences will come from the existing Technology Services Budget. Spending the Technology Services Budget on these security items may mean that other projects are pushed back into following years, such as the internal infrastructure upgrade.

7.2 There are no staffing consequences arising from this report.

8 Legal Considerations and Implications

8.1 There are no legal considerations or legal implications arising from this report.

9 Risk Assessment

9.1 There is a risk that if we don't take out Cyber Insurance and have a serious Cyber Security Incident that we may not be able to recover costs related to systems downtime and associated losses incurred by the Council.

9.2 Given that we may be able to recover some costs or losses associated with a Cyber-attack through other insurance policies we have in place, the risk is deemed to be low.

9.3 Even if we have Cyber Insurance, we may not be able to claim back as much of the losses as we have paid out in premiums. This would mean that the policy is effectively worthless.

10 Procurement implications

10.1 There are no procurement implications arising from this report.

11. Equalities and Human Rights implications / Public Sector Equality Duty

11.1 There are no equalities and Human Rights Implications arising from this report.

12 Environmental Implications

12.1 There are no environmental implications arising from this report.

13 Other Considerations

13.1 Cyber Security incidents in most cases lead to a data breach which then brings in GDPR/Data Protection. Having Cyber Insurance or not is immaterial to the Information Commissioners Office (ICO) when investigating a Data Protection incident.