

## PFCC Decision Report

<b>Report reference number:</b> 089-2021
<b>Classification</b> (e.g. Not protectively marked/restricted): Not protectively marked
<b>Title of report:</b> Cyber Cover Update
<b>Area of county / stakeholders affected:</b> Countywide
<b>Report by:</b> Matt Tokley, Corporate Accounting Manager
<b>Date of report:</b> 3 <sup>rd</sup> June 2021 (updated 16 <sup>th</sup> June 2021)
<b>Enquiries to:</b> Matt Tokley

### 1. Purpose of the report

- 1.1 To approve the preferred way forward in respect of cyber cover for the force, and to note the reasoning for the proposed delay in acquiring this cover.

### 2. Recommendations

- 2.1 The PFCC is recommended to:

Approve the attached report which sets out a proposal to progress with looking into acquiring specialised cyber insurance cover, but to defer this until such a time that the force has assurance that market conditions are beneficial to progress and purchase this cover, and using the PFCC's insurance broker Marsh to advise on the options available.

### 3. Benefits of the proposal

- 3.1 To acquire specific cyber-related insurance cover which the force currently lacks, following a review and assessment that steps need to be taken to further mitigate this ever-increasing area of risk. Delaying the proposal and potentially looking to participate in a South East and Eastern Region Procurement Insurance Consortium (SEERPIC) market exercise and / or considering a solution via the Police Digital Services Team will see the force benefitting from economies of scale and achieving cost savings in comparison to the current cover options available.

#### **4. Background and proposal**

- 4.1 Cyber security involves the protection of internet connected systems (including hardware, software and associated infrastructure), the data on them and the services they provide from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally as a result of failing to follow security procedures or being manipulated into doing so.
- 4.2 Following discussion with SEERPIC partners and a review of risks within the insurance sector it has been identified that cyber security is an area of emerging importance worldwide, with several high profile examples in the public sector in recent years.
- 4.3 In May 2017, the NHS was seriously disrupted with more than 80 hospital trusts and 8% of GP practices impacted, after ransomware was used to lock down hospitals in England. The subsequent financial impact has been estimated at circa £92m, £20m relating to lost output and a further £72m of I.T. support to restore data and systems. In February 2020 a further high-profile incident occurred at Redcar and Cleveland Borough Council. About 135,000 people were without online public services when the authority's website and computers were targeted, and the estimated cost was in excess of £10m. Hackney Council was also the target of a serious cyber attack that affected its I.T. systems and services in October 2020, with a similar liability of circa £10m. The reputational impact of such breaches on an organisation can also be extremely damaging.
- 4.4 As the force does not have any specific cyber insurance cover, a recommendation was made to Chief Officers and the PFCC to give the go ahead for discussions with the SEERPIC approved broker (Marsh) to look at potential options to acquire cover, and the potential best routes to provide this. This recommendation was approved at the March 2021 Strategic Board meeting and a subsequent fact-finding exercise has been undertaken internally, setting out the current systems and controls in place across the force, as well as exploring the options in the market.
- 4.5 Based on an updated assessment of the recommended specialist provider within SEERPIC, concerns have been articulated that the market is expected to see significant price rises as providers capitalise on the growing demand for this specialist cover. In addition, the requirement for penetration testing, whereby an attempt is made to deliberately breach an organisation's systems, means there are some serious drawbacks and concerns in respect of proceeding with cover at the current time. It is therefore proposed to seek further discussions within SEERPIC, with a recommendation that a joint proposal is submitted for cover to be put in place from October 2021, which would be consistent with the timing of the force's other insurance policies.

#### **5. Alternative options considered and rejected**

- 5.1 Whilst accepting that prevention is still the main objective in relation to cyber risk, the acquisition of cover arrangements is on balance still recommended to provide assurance to the PFCC. However, a decision to proceed with acquiring cyber cover from the current preferred provider used by the SEERPIC broker would mean potential exposure to cost increases as well as security and access

risks which would not be acceptable for the force or its I.T. controls and related polices / procedures. Furthermore, it is noted and accepted that existing I.T. controls within the force are robust and secure, particularly with the recent implementation of Office 365 technology. Therefore, whilst it is acknowledged that cyber cover is an area of importance which needs a solution as soon as possible, the time is not currently right to take out this cover, and existing controls already mitigate any potential material risk. Instead, further research and exploratory work is recommended to be undertaken.

## **6. Police and Crime Plan**

- 6.1 All of the priorities and workstreams identified within the Police and Crime Plan are underpinned by the need for the force to deal with large amounts of data and information, much of which is sensitive and confidential, and relating to criminal investigations. It is therefore paramount that systems are robust and secure, with exposure to emerging threats nullified by appropriate controls which are suitable to deal with the level of risks required. Where it is not feasible to protect due to the rapid progression of new threats which override these controls, cyber cover will provide further assurance to the force in respect of compensatory options, should this ever be required.

## **7. Police operational implications**

- 7.1 The force's I.T. systems are fundamental to operational policing including Athena, Storm, Office 365 and Mobile First technology such as ESMCP. Failure of these systems or breaches of security could fundamentally impact operational activity with serious consequences, including financial losses and the inability for the force to undertake core policing activity within a specified time period.

## **8. Financial implications**

- 8.1 It has been estimated that the proposal to proceed with cyber cover at the current time could lead to the force incurring price rises of between 20 – 40% compared to current premiums being paid by SEERPIC partners. It is therefore proposed to defer purchasing this cover until assurance has been obtained about the future direction of this specialised market. The force will use the approved SEERPIC insurance broker to ensure best value is achieved within the market.

## **9. Legal implications**

- 9.1 There are no specific legal implications with the recommendation although the PFCC is advised to note the additional risks that could arise following a cyber incident, including legal claims against the force from those impacted. Ensuring sufficient legal protection is in place is an underlying priority in respect of the reasoning for acquiring this cover.

## **10. Staffing implications**

- 10.1 There are no specific staffing implications. However, the potential staffing and resourcing issues should the force be required to react and recover from a cyber-related incident could be hugely significant and very costly to the force.

**11. Equality and Diversity implications**

11.1 There is no significant impact of this decision report in respect of issues relating to equality, diversity or human rights.

**12. Risks**

12.1 The risks of not taking out cyber cover are set out within this decision report as well as the related report. The period of lockdown caused by the COVID pandemic means there has been a sharp rise in online-related crime, which has progressed significantly in a very short space of time. Failure of organisations to react effectively to this growing area of crime could potentially have serious operational and financial consequences should such threats manage to override the protection already in place within existing systems.

**13. Governance Boards**



13.1 The original Insurance Update paper, which included the cyber cover recommendation, was presented to the Chief Officer Group of the Chief Constable on 10<sup>th</sup> February 2021, and the PFCC's Strategic Board on 11<sup>th</sup> March 2021. This update was presented to the Chief Officer Group on 2<sup>nd</sup> June 2021 and to the PFCC's Strategic Board on 10<sup>th</sup> June 2021. This version of the decision report has been updated to add extra detail.

**14. Background papers**

14.1 The key background papers are the earlier reports submitted as per 13.1.

**Report Approval**

The report will be signed off by the OPFCC Chief Executive and Treasurer prior to review and sign off by the PFCC / DPFCC.

Chief Executive / M.O.	Sign:	
	Print:	P. Brent-Isherwood
	Date:	27 September 2021
Chief Finance Officer / Treasurer	Sign:	
	Print:	..... Julia Berry .....
	Date:	..... 27 September 2021 .....

**Publication**

<b>Is the report for publication?</b>	<b>YES</b>	<input checked="" type="checkbox"/>
	<b>NO</b>	<input type="checkbox"/>

**If 'NO', please give reasons for non-publication** (Where relevant, cite the security classification of the document(s)). State 'None' if applicable)

.....N/A.....  
.....

If the report is not for publication, the Chief Executive will decide if and how the public can be informed of the decision.

**Redaction**

If the report is for publication, is redaction required:

1. Of Decision Sheet?	YES	<input type="checkbox"/>	2. Of Appendix?	YES	<input type="checkbox"/>
	NO	<input checked="" type="checkbox"/>		NO	<input type="checkbox"/>

If 'YES', please provide details of required redaction:

.....  
.....

Date redaction carried out: .....

**Treasurer / Chief Executive Sign Off – for Redactions only**

If redaction is required, the Treasurer or Chief Executive is to sign off that redaction has been completed.

Sign: .....

Print: .....

**Chief Executive/Treasurer**

**Decision and Final Sign Off**

I agree the recommendations to this report:

**Sign:**  .....

**Print:** Roger Hirst

**PFCC**

**Date signed:** 17 November 2021

I do not agree the recommendations to this report because:

.....  
.....  
.....

**Sign:** .....

**Print:** .....

**PFCC/Deputy PFCC**

**Date signed:** .....