PFCC
POLICE, FIRE AND CRIME COMMISSIONER FOR ESSEX

Police Fire and Crime Commissioner for Essex
Essex Police Strategic Board

Title of Report / Agenda Item	Cyber Insurance
Document Classification	Official
Date of PFCC's Strategic Board meeting	14th December 2021
Agenda Number	3iv)
Chief Officer	DCC Andrew Prophet
Author on behalf of Chief Officer	Matt Tokley, Head of Corporate Accounting
Date paper was written	3rd December 2021
Version Number	V1.0
Date of approval at COG (or other named meeting or person authorising)	Extraordinary COG meeting (7th December 2021)
Date Approved by Essex Police Finance Department	3rd December 2021

1. Recommendations

The Strategic Board is asked to recommend to the PFCC that the proposal to acquire cyber insurance cover is progressed with a solution in place by no later than the end of January 2022, based on the explicit threat this risk poses.

It is recommended that subject to the ongoing work required before a formal cyber proposal can be confirmed (which will be reviewed again by COG in January) a formal decision sheet will be submitted to the PFCC to enable cover to be enacted as soon as possible after the start of February 2022.

It is recommended that the initial policy will be for a part-year period in year 1, up until the 30th September 2022 so this policy aligns with the other insurance cover in place across the force. Thereafter, all policies will be renewed and run annually from 1st October 2022 onwards.

Based on the final terms of the insurance contract not being confirmed at the current time, no decision sheet has been submitted with this report, and this will instead follow after Christmas as per the process set out above.

2. Executive Summary

This is a paper following up on the previous recommendations highlighted to the PFCC in respect of looking into a cyber insurance solution for the force, in view of the significant upturn in frequency, size and scope of cyber claims. The paper sets out a proposal to explore a route in which cyber cover will be potentially procured for the force, subject to an external assessment of the controls and systems in place.

The force has engaged JLT to assist with the identification of a best-fit cyber insurance solution and a market exercise is currently underway. Due to the nature of this cover insurance providers typically request to test controls in place prior to offering cover. This is in the process of being arranged with the support of colleagues in the IT team to ensure data sharing processes are managed sensitively. Once this exercise has been completed draft terms of cover should be forthcoming, at which point a final proposal will be submitted for approval to the PFCC.

3. Background

Overview

Cyber risk relates to the risk of damage to an organisation through its information systems. It is any risk associated with financial loss, disruption, or damage to the reputation of an organisation from failure, unauthorised or erroneous use of its information systems.

Cyber risk may come from various sources including cybercrime, cyber terrorism, corporate espionage, faulty safety controls and insider threats. These risks can manifest themselves in various ways, both internal and external.

External cyber risk is any risk that comes from outside the organisation and often represent the most commonly known threats when the term ‘cyber risk’ is used. Some of the most well-known examples of external cyber-attacks include phishing (a social

engineering attack trying to deceive the user or recipient), malware (malicious software) and ransomware (a type of malware that locks a user out of their information systems).

Whilst external threats provide a great risk to any organisation up to half of all known breaches are typically internal, involving insiders or third-party partners. Whilst malicious intent from insiders continues to be widespread, this element is on the decline and it is actually employee and third party mistakes which are now more common in this category. These issues include misconfiguration of systems and servers, unpatched software as well as lack of training. Often an employee who hasn't been trained in proper cyber hygiene can open up an organisation to an external threat.

Whilst technology has evolved quickly due to the need to change processes in line with new ways of working following the COVID-19 pandemic, the controls around these new processes have not always kept up with the rapid change. In addition, criminals targeting such technology have got smarter and more knowledgeable of how they can manipulate these systems.

The recently updated general data protection regulations (GDPR) have reinforced the need to protect information while highlighting the remedies available to organisations affected by data breaches. At the same time cyber criminals have become increasingly sophisticated in their attempts to target both personal and organisational information, and system attacks now continue to be reported on an almost daily basis, with the threat at organisational level now significant.

Cyber-attacks in the public sector

There have recently been some high-profile cyber-attacks in the public sector which have highlighted the risks and potential impacts which could arise for other organisations in similar situations.

In February 2020 a cyber-attack on Redcar and Cleveland Borough Council's computer systems is estimated to have cost more than £10m, with government support needing to be requested to assist with the financial pressures which subsequently arose. About 135,000 people were without online public services when the authority's website and computers were targeted. At the time of the attack the council had industry standard tools deployed to secure its computer network, which had been configured to provide optimum protection. These were in accordance with the standards set out by the Public Services Network (PSN). However, the lack of specific cyber-defences meant that the attack was able to succeed. Ultimately nearly £2.5m of the resulting costs related to the extensive recovery and replacement work to the council's IT infrastructure and systems.

Hackney Council was also the target of a serious cyber-attack that affected its IT systems and services in October 2020. Again, the costs have been estimated in excess of £10m, a similar level of investment to that required by Redcar & Cleveland. The attack, undertaken by organised criminals, related to a specific ransomware tool and rendered key financial and operational systems inaccessible and paralysed several council services, including its ability to make and receive payments, and take housing waiting list applications. Again, specific tools to counter such cyber-crime activity had not been purchased by the authority in question leaving them open to sophisticated criminal activity.

The above examples represent what can happen when organisations are not adequately prepared for cyber-crime activity. If a relatively small council can incur a £10m hit what could be the potential impact for an organisation the size of Essex Police,

with its breadth of information systems? The reputational impact of such a breach on an organisation can also be extremely damaging and merits serious consideration.

Cyber Security

It is widely accepted that organisations are being actively targeted by cyber criminals each and every week and it is therefore paramount that basic security measures are in place. 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.

Cyber security involves the adoption of a wide range of measures to try and minimise the impact of cyber risks impacting an organisation. The most common element of these tools are software packages to mitigate 'application security' threats, a common point of intrusion for cyber criminals. Such tools include anti-malware and anti-ransomware software, as well as the use of firewall technology. Also used are 'network security' measures including encryption and sophisticated passwords which need to be regularly changed and follow a format which cannot be easily replicated.

Further measures include more people-orientated techniques of cyber-crime prevention. These elements include a focus on staff training and awareness, showing how security threats can affect them and their work and to ensure a focus on applying best practice at all times. Leadership commitment is also key to cyber resilience. Without it, it is tough to establish or enforce effective processes. Management must be prepared to invest in appropriate cyber security resources, such as the aforementioned awareness training.

Whilst cyber security techniques effectively mitigate and block the impact of a wide range of cyber-crime activity, they are nonetheless not full proof nor a solution which eliminates the threat of this risk. Furthermore, the nature of this criminal activity means the threat is constantly evolving, with security procedures often behind the curve in this respect e.g. a reactive solution. Based on the impacts which other organisations have experienced it is therefore nonsensical not to explore further options as to how Essex Police could protect itself against cyber criminals directly targeting the organisation.

In addition to the ongoing threat of new sophisticated cyber-attacks which cannot always be understood or prevented, another big threat to organisations is the business interruption and recovery processes which need to be initiated immediately after such an event occurs. As the examples of Cleveland and Redcar, and Hackney demonstrate, often the attacks in question have a fundamental impact on front line services to the public and related systems. The costs and time needed to resolve such attacks are often extremely large for organisations, and typically form the second highest element of costs in such instances, second only to the subsequent IT solutions purchased themselves.

4. Options and analysis (to include proposals, benefits, alternatives)

Cyber Insurance – Overview

The cyber market remains extremely challenging – for a number of years this cover has been widely available at a very reasonable price however, this is no longer the case. In addition to the general insurance market hardening over the last two years, cyber has seen a high number of losses including some of significant value which has led the

market to contract and reduce available capacity.

In addition to increasing the cost of cover, there has been some reduction in the scope of cover available. Quite simply, there is far less competition available. Furthermore, insurers are now extremely selective in choosing which risks to quote upon and minimum security requirements are generally required before an insurer will provide terms.

There is a public sector aspect also driving the lack of insurer appetite – by the nature of the organisation (and particularly police forces) the data held is voluminous and very sensitive, meaning the exposures in the event of a loss are high. Additionally, many public sector organisations have not had sufficient precautions in place (from the market's perspective) and there have been some big ransomware type incidents. However, as the Police are required by the Home Office to have such stringent controls in place it is paramount that this aspect is made clear to insurers – the risk is that if not, then the Police are 'tarred with the same brush' as other public sector entities.

Specialist covers such as cyber have been around for some time now, mainly in respect of third party exposures, which account for the majority of the specialist market. A small but increasing number of underwriters are now offering first party cover. This is an area subject to fairly constant change as risks increase and new risks come onto the market. Cyber is very much at the forefront of these type of covers and certainly fits the profile for how these specialist covers are structured and constantly evolving.

It is also important to appreciate the difficulties insurers are having in understanding and quantifying exposure to cyber risk – one malware attack can lead to thousands of organisations being impacted around the world. There is also increased awareness of aggregation events and supply chain risk. In view of these risks underwriters are now looking to satisfy their understanding of a number of key controls of the client, before giving consideration to providing insurance quotations. This process is known as 'penetration testing' or alternatively 'non-evasive scanning'.

The scope of cyber insurance must also be considered. Essentially the name 'cyber' insurance is somewhat of a misnomer, referring as the name suggests to IT-related activities and risks. In fact the cyber insurance essentially protects against all data loss, not just that held on electronic devices or systems such as laptops, computers, tablets or mobile phones. This means that paper files would also be within scope, thus covering such eventualities as documents being left or lost in the public domain, or information being shared with third parties in error. By acquiring such cover organisations are therefore protected against a much wider breadth of risks than immediately assumed.

When taking out cyber cover the applicable retention, threshold and deductible levels will need to be considered. These include the standard 'liability' deductible per claim, a busines interruption and data recovery loss deductible per incident, as well as a breach response standard excess. In addition other terms will need to be considered including the waiting period for an insurer response as well as a notified persons threshold, which again links into business continuity-related workstreams.

What is typically excluded within cyber insurance policies are 'acts of war' e.g. deliberate and focused criminal activity targeting data, which is undertaken by state-run entities as opposed to individuals or smaller-scale criminal groups. Whilst this would seem to be a remote eventuality, a police force or any public sector organisation may be seen to be a legitimate target in their role as a strand of UK government and the provision of public services.

Cyber insurance will also provide organisations with the peace of mind that if things do go wrong with their data, the insurer will assist in the recovery process of both their data and their front line services. Immediate specialist assistance will be on hand to review the issues and advise on ways forward, working closely with strategic teams to put localised business continuity plans into action. There will often be a significant administration burden in such instances, with call centre facilities often needed to link in with a wide range of stakeholders, both internal and external to the organisation. This service can also be provided within the cover package, meaning the organisation is not only protecting its data but limiting the impact on its front-line services being impacted.

Cyber Insurance – Essex Police

To reiterate, the force does not currently have any specific cyber insurance cover in place. This topic has been previously flagged to Chief Officers as a risk to the force, with a proposal that a cyber insurance solution is actively explored and ultimately procured. At the current point in time four of the ten SEERPIC forces have specific cyber cover, Norfolk and Suffolk, and Surrey and Sussex. Essex are therefore one of the remaining six forces (including Kent) who do not have this cover.

The force has actively engaged the SEERPIC consortium brokers JLT to assist with the identification of a best-fit cyber insurance solution. The starting point for this work has been a data gathering exercise to summarise systems and controls currently in place across the force as well as a wide range of supplementary information in respect of IT-related processes. This work has involved the Insurance team liaising with IT colleagues with this information being collated and shared with JLT.

As JLT now have the responses to the questions posed in respect of minimum requirements the market has now been approached to seek quotes. Whilst this market remains limited there are a few potential insurers who will be interested in quoting for this cover and it is highly likely that Beazley (who also provide the cyber cover for the four insured SEERPIC forces) will provide the most cost-effective solution. Beazley have been an existing provider in the cyber area for some time, and they are viewed as a market specialist for this type of cover. Should the force follow this route it would also benefit from the insurer already having a sound understanding of the risk profile of four fellow consortium partners. Furthermore, it is likely that JLT would also recommend this provider on the basis that the covers would then be broadly consistent with the fellow SEERPIC forces and given their well-established market position and previous experiences in the sector, should provide competitive terms.

It should nevertheless be noted that the wider market position will still be comprehensively reviewed and if a more suitable quote is on the table these options will be fully evaluated to assess their relative advantages and disadvantages. Ultimately it will be a blend of the most economically advantageous and the most operationally acceptable cover option which will be the preferred choice for the force.

As expected, JLT have advised that it is most likely that a non-invasive scanning test will be required before terms can be prepared. In particular, Beazley specifically require this and it was therefore a requirement for the other SEERPIC forces before their cover was agreed. Quite simply, if the force doesn't agree to having this done (or if we agree but the findings are poor) then Beazley will not offer terms. It is therefore proposed that discussions with the other four SEERPIC forces would be useful to review what this process entails and how any concerns that they had at the outset were ultimately allayed. A subsequent request has also been lodged with IT to identify the domain names for which such an exercise would require, and this is currently being followed up.

The controls that JLT have requested responses for are as follows:-
- MFA (multi-factor authentication) for remote and admin access
- Endpoint detection and response
- Process or protocol for applying critical patches
- Secured offline backups
- Remote desktop protocol is not exposed outside the firewall
- Privileged access management
- E-mail filtering and validation process
- End of life systems (replacement policy)

In respect of costings it is difficult to indicate what the premium for Essex would be as each request for cover is individually assessed based on many factors including the number of records, the sensitivity of the data and the security arrangements in place. Also, the policy limit set and any deductibles will also be of relevance. This is further complicated by the fact that the pricing rates are generally on the rise. However, what can be used as a basis and estimate for the costings is the premium range for the four other SEERPIC forces who already have this cover. This range is £36k-£43k per annum, with 12% insurance premium tax (IPT) chargeable on all of these premiums (a non-recoverable tax). It would therefore be a reasonable assumption to assume that the force could procure a cyber insurance solution in the region of £50k per annum (pro-rata for the 2021/22 insurance period).

It should be noted that specialist covers have increased significantly over the previous twelve months with JLT estimating that forces with this cover saw increases of between 50-60% at the last renewal date. This is reflective of the general trend of organisations holding more and more data (e.g. more data = more risk) as well as the constantly evolving landscape of this type of crime, which insurers need to spend more time with their underwriters on to understand and quantify the associated risks arising.

Whilst the cost increases suggest that the force may therefore see immediate premium increases when the next renewal period comes round in October 2022, it should be noted that updated IT technology within an organisation will substantially assist in the view the insurer takes of a new potential client. In respect of Essex Police, the substantial investment in the IT capital programme including the Office 365 rollout and SharePoint workstreams, means that data loss risks would be substantially reduced from the insurer perspective, and should directly lead into premiums not increasing significantly at the next renewal period. This would therefore be comparable to the motor insurance risk-related workstreams where Edison (the insurer) have required SEERPIC forces to meet various objectives in respect of risk reduction processes to ensure the onward provision of cover is not impacted, nor material rises in premiums being passed on to clients. Such workstreams may potentially be an onward requirement in the make-up of a cyber insurance policy for the force.

Deductibles will need to be considered as well as maximum thresholds for sums insured. Based upon an assessment of similar customers currently in this market it is anticipated that a breach response deductible will be in the region of £10,000 per incident, with a liability and business interruption deductible of circa £25,000-£30,000 per incident.

Whilst JLT have approached the market on behalf of the force, it should be noted that there is no guarantee that terms will be offered and if they do, the costs may be high. Furthermore, once the cover has been purchased, it may well be that the market deteriorates further and if so additional challenges could be foreseen at the next renewal date.

Next Steps

The information supplied by the IT department in order that a quote can be prepared, is currently with the SEERPIC brokers JLT. Upon review of this information it is expected that further queries will be received which will need to be answered by the Insurance team, thus adding a potential week or so into the timeline.

Based on discussions with internal colleagues, national partners and IT advisors the Chief Information Officer of Essex Police has expressed some concerns with the proposed 'evasive scanning' processes required to obtain a quote. In order that these concerns are allayed JLT have recommended that further assurance and clarification is received from Suffolk Police in respect of these scanning procedures. An initial response has subsequently been received indicating that the terms used (vulnerability testing, penetration testing etc) is not necessarily what the process appears to be, and it is more to do with open source research against the organisation to ascertain what is in the public domain. This effectively means that the proposed testing against networks and infrastructure may not actually be required in its physical form, and it would instead constitute more of a discussion, research and information-gathering process. In view of this feedback, discussions are currently underway with JLT to confirm whether this process would be similar for Essex, and assuming the outcome of this consultation is acceptable to the force, it is envisaged that the 'scanning' work could be scheduled before Christmas to enable a quote to be received in early January.

Once an initial proposal has been received the Insurance team will review the terms of the cover to satisfy itself that the deductible levels and cover thresholds are proportionate and adequate for the risks required to be covered. Two or three options where differing levels of risk will be accepted, will be reviewed to compare value for money. Where appropriate, the Insurance team will link in with IT colleagues to understand potential impacts.

Once the terms of the final quote have been deemed to be acceptable, and approval is given to proceed with the acquisition of this cover, it is proposed that a part-year policy is acquired from the start of February 2022 up until 30th September 2022, thus aligning this policy with the other covers in place for the force. The only weakness of this approach would be that the period of time which would elapse before the next renewal date would be less, thus the force would be exposed to potential market-led increases more quickly.

Going forward the use of and requirement for cyber insurance will continue to be monitored and reviewed as IT systems evolve and the associated risks change. It is hoped that with technological advances in IT that the threat of cyber-crime will slowly reduce, thus allowing more traditional insurance covers and cyber security measures to be sufficient for threats of this nature.

In summary, for the time being cyber risk is not going away and if anything is becoming a more prominent risk across the sector. Whilst investment in IT technology for the force remains substantial, and related controls are robust and secure, the proposed costs of taking out this specialist cover appear to be immaterial compared to the potential risks of a cyber incident occurring. In the rare event of an incident being at a significant level and controls are breached, the organisation would be exposed to a major cyber-attack with wide-ranging and damaging consequences. On this basis, it is therefore proposed that cyber cover is purchased at the earliest possible opportunity.

In view of the current situation whereby terms are still awaited from the insurer as well as further assurance currently being sought by the Chief Information Officer in respect of

the insurer's demands, it is proposed that this paper is for noting only at this point. A decision report will then be submitted to the PFCC during January ahead of the proposed insurance cover commencement date of the 1st February 2022. Whilst this means that the PFCC Strategic Board in December will not directly endorse the decision to procure this cover, it will nonetheless agree the route for the way forward and receive clarity on the proposed structure and expected costings of the cover recommended. The decision to proceed will then be able to be formally approved during the Chief Constable's 1-2-1 meetings with the PFCC.

5. Risks and Mitigations

The risks of not taking out cyber cover are set out within the case studies in section 3 of this report, as well as the emerging risks covered in this element of the 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 for 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.

6. Links to the Police and Crime Plan

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 provide adequate protection 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. Financial Implications

It has been estimated that the proposal to proceed with cyber cover at the current time will equate to an annual premium equivalent of approximately £50k per annum. This is based upon a broad assessment of the current market, as well as the costs which other SEERPIC forces are currently paying. It should be noted that due to the volatile insurance market and ever-challenging risks for this particular type of cover, premiums could substantially increase at future renewal dates. If these price rises do occur the force will need to continue to review the value for money of retaining this cover compared to the level of threat and risk which cyber currently poses. It is proposed to defer purchasing this cover until a full assessment has been completed in respect of the best option available, with the force using the approved SEERPIC insurance broker (JLT) to ensure optimum value is achieved within the market.

8. Legal Implications

There are no specific legal implications with this 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. Furthermore, as stated elsewhere within this report there is an understanding that this insurance covers data loss and data protection in broader formats, rather than just IT-related. In such scenarios the force would potentially have more robust protection in place for any GDPR legislation-related legal claims which may arise in the future.

9. Staffing Implications

There are no specific staffing implications or related costs of acquiring this cover. However, it should be noted that 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. In such scenarios call centre and disaster recovery/business interruption resources would be supplied as part of the cyber cover package, thus ensuring recovery processes are structured and managed effectively, with normal operations returning to normal at the earliest possible time.

10. Equality and Diversity Implications

There are no specific equality or diversity implications of this proposal. The related process to identify a supplier in the cyber market will be undertaken free of bias and prejudice, and be based upon an assessment of the best supplier in the marketplace, using a set of value for money and quality-based criteria.

11. Police Operational Implications

The force's IT systems are fundamental to operational policing including Athena, Storm, Office 365 and Mobile First technology such as ESMCP. Failure in the operation or use of these systems and/or related 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.

12. Governance Boards

- Insurance Update report, PFCC Strategic Board, 11th March 2021
- Insurance Update report, PFCC Performance & Resources Board, 29th November 2021

13. Future Plans (long-term strategic direction)

The proposal is in line with the long-term strategic direction of the force of ensuring that emerging risks are identified, managed and mitigated in the most effective way possible.

14. List of background papers and appendices

Please refer to the papers (and accompanying decision reports where applicable) for the two previous governance boards, as referred to in section 12.
