LFB
LONDON FIRE BRIGADE

Decision title

Cyber Defence System

Recommendation by
Chief Information Officer

Decision Number
LFC-0006-D

NOT PROTECTIVELY MARKED

Summary

Report LFC-0006 makes the case for the Brigade to procure a "Cyber Defence System", to be deployed to protect the Brigade's information, systems and associated assets from hostile / malicious threats.

Decision

The London Fire Commissioner delegates the approval for the procurement initiation for a Cyber Defence System to the Director of Corporate Services.

Dany Cotton QFSM
London Fire Commissioner

Date 23/4/18

Access to Information – Contact Officer	
Name	Steven Adams
Telephone	020 8555 1200
Email	governance@london-fire.gov.uk

LONDON FIRE BRIGADE

Report title

Cyber Defence System

Report to London Fire Commissioner	Date 11 April 2018
Report by Chief Information Officer	Report number LFC-0006

NOT PROTECTIVELY MARKED

Summary

The paper makes the case for the Brigade to procure a "Cyber Defence System", to be deployed to protect the Brigade's information, systems and associated assets from hostile / malicious threats.

Recommendation

The London Fire Commissioner delegates the approval for the procurement initiation for a Cyber Defence System to the Director of Corporate Services.

Background

1. In recent years the security threat posed to organisations around the globe from cyber attacks, malware and associated threats, has increased exponentially. Most of us will remember only too well the "WannaCry" ransomware attacks that took place last year.

2. On May 12th 2017, security companies noticed that a piece of malicious software known as WannaCry was spreading across the internet, first in the UK and Spain, and then around the world. It would reach 230,000 computers in 48 hours, an unprecedented scale of infection according to Europol, Europe's international police agency.

3. WannaCry rendered useless some of the computers that help run Britain's National Health Service (NHS), causing ambulances to be diverted and shutting down non-emergency services. It also infected machines at Telefónica, Spain's biggest telecommunications company; at Hainan, a Chinese airline; and even in Russia's interior ministry.

4. However, whilst WannaCry was perhaps one of the more high profile attacks, it was one of a number of attacks that have been perpetrated since the early 2000's and was not actually the worst. Other worms—Conficker, MyDoom, ILOVEYOU—caused billions of dollars of damage in the 2000s.

5. There is no reason to believe that the threat to systems around the world will do anything other than increase. Whilst the Brigade has multi-layered defence systems already in place such as anti-

virus scanning, web-filtering and a strategy to implement security patches regularly, we currently lack an overarching cyber defence system.

6. The Brigade itself was unaffected by the WannaCry ransomware. This was due in no small part to the efforts of ICT staff who worked constantly over the weekend in question to ensure that we had taken all reasonable precautions to protect systems against this treat. This included isolating the Brigade from the internet for a period of time.

7. The Brigade is looking to take positive action in relation to the ever-changing cyber threat and this will include adhering to the "cyber essentials" guidance published by the National Cyber Security Centre - NSCC and potentially seeking accreditation against the cyber essential plus standard (external accreditation).

8. However, as the nature and frequency of threats evolve and increase, it is clear that we need to adopt a more proactive stance and establish a "cyber defence system" to minimise the chances of Brigade operations being impacted by potential future cyber attacks.

Requirements

9. The Brigade had initially identified a need to deploy a "Security Information and Event Management System" – 'SIEM'. Such systems combine security information management with security event management into one system, hence the name SIEM (pronounced 'sim'). Many organisations around the world have either installed such a system or are planning to do so.

10. Although SIEM propositions from different suppliers may vary their approach, they all share an underlying principle. That is to aggregate relevant data from multiple sources, identify deviations from an established "norm" and to take appropriate action. For example, when a potential issue is detected, a SIEM might log additional information, generate an alert and instruct other security controls to stop an activity's progress.

11. Most SIEM systems work by collecting information from a range of collection agents deployed on a network. Security related event information may be collected from end-user devices, servers, network equipment, as well as specialised security equipment like firewalls, antivirus or intrusion prevention systems.

12. However, SIEM systems can be very resource intensive. Once data has been collected and collated, manual intervention is regularly required to determine an appropriate course of action to be taken.

13. The latest generation of cyber security products, encapsulate the approach detailed above but then go onto take this to the next level. Using "machine learning" algorithms, these products are able to operate unsupervised (to a large extent) are able to identify, classify, prioritise and neutralise malware and advanced persistent threats (APT), using built in artificial intelligence (AI) type processes.

14. This means that rather than operate on logs, these next generation systems monitor raw network traffic, seeing every single device and user, and automatically learning the complex relationships between them. Having initially established a detailed understanding of what "normal" looks like, these systems can identify emerging threats that have bypassed traditional defences, and are active within the network

15. Whilst these next generation systems may be more expensive than traditional SIEM systems, the system cost really needs to be looked at in the context of the cost of a recovery from a cyber breach / ransomware ware attack.

16. There are numerous accounts of organisations having to spend considerable amounts of money in clean up operations from cyber attacks / ransomware outbreaks (and that is only the ones that are reported). For example, shipping giant and NotPetya victim Maersk was forced to replace tens of thousands of servers and computers in the aftermath of a recent ransomware attack. The cost to the business in terms of both operational and reputational loss was immense and in financial terms, far more than the anticipated cost of a defence system.

17. Whilst no system is able to offer a guarantee against evolving cyber threats, these new generation systems are better equipped to deal with "zero-day" attacks (A zero-day exploit is an attack that exploits a previously unknown security vulnerability. A zero-day attack is also sometimes defined as an attack that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known).

18. The Brigade does not have a large security team and therefore cyber defence products that minimise day to day direct supervision and offer the ability to detect and prevent zero-day attacks will be particularly attractive. The introduction of such a system within the Brigade will provide us with a real opportunity to be on the front foot in the constant battle against persistent and unpredictable cyber attacks.

Finance comments

19. In line with the Brigade's ICT strategy, the preference is to procure a cyber defence product as a service, financed from revenue rather than capital expenditure. Essentially this makes the procurement a "pay as you go" service (rather than one where payment is all upfront and a capital bid required in the future to replace it), which itself will provide opportunities for the Brigade to switch to alternate products in the future.

20. Actual costs will not be known until a tender exercise has been completed, but soft market investigations have been undertaken to ensure that sufficient budgetary provision be made for this type of service. It is anticipated that we would seek to enter into a three-year contract for this service.

21. Whilst the introduction of a cyber defence system does not offer any immediate cost savings, there are potential avoided costs in terms of not having to ask staff to work constantly over a weekend if there were to be a further widespread attack. In addition, the cost of a "cleanup" operation post a successful attack could be huge in comparison to the financial outlay for such as product.

Collaboration Opportunities

22. We are currently exploring collaboration opportunities across the group and throughout the Fire Service. Meetings have taken place with both Transport for London (TfL) and the Metropolitan Police Service (MPS) in respect to this requirement. TfL were very helpful and it was useful to understand their setup and approach. However, there are no obvious collaboration opportunities with them at present. The system that they use demands a large team to analyse the information produced which is the scenario that we are trying to avoid.

23. The MPS are piloting a system that would seem to meet our requirements, in so far as it uses AI / machine learning. We have agreed to contact them again around the end of April so that we can consider their feedback, and note any lessons learned.

24. The Greater London Authority (GLA) and London Ambulance Service (LAS) have asked for details of the requirement, and the Chief Information officer has shared a statement of requirements with them. This will be followed up in the coming weeks.

25. Depending upon the direction that the MPS take, there is the possibly of some form of group collaborative procurement.

Timeline

26. The intention would be to initiate a procurement in April or May 2018, with implementation around June/July 2018.

27. It is important to note that LFB will be specifying as part of the procurement process, that any product selected will be subject to a three month "live trial". This is specifically to allow us to make a determination in a real-world situation about the amount of security staff resource that needs to be allocated to the product.

Workforce comments

28. There are no plans for staff-side consultation.

Legal comments

29. General Counsel has reviewed the report and notes that any procurement will need to be carried out in accordance with the public contracts regulations and the Commissioner's Scheme of Governance, and that exploring collaboration with other emergency services, where this would improve their efficiency or effectiveness, is consistent with the Commissioner's duty to collaborate under the Policing and Crime Act 2017.

Sustainability implications

30. There are no sustainability implications.

Equalities implications

31. There are no equality implications attached to the content or recommendation detailed in this report.

List of Appendices to this report:

There are no appendices to this report.