

# Report – Police Committee

## Cyber Security Strategy

*To be presented on Thursday, 21st June 2018*

*To the Right Honourable The Lord Mayor, Aldermen and Commons of  
the City of London in Common Council assembled.*

### SUMMARY

The City of London's financial and professional services (FPS) industry faces a unique cyber threat and, as a sector designated as Critical National Infrastructure, there is a need to enhance its protection from future attack.

The City of London Police (CoLP) and the Economic Development Office (EDO) therefore propose to partner to develop and deliver a cyber strategy incorporating:

- the 'Cyber Griffin' initiative, which will include expert briefing, training and scenario planning to help businesses in the Square Mile defend against cyber-attack;
- a cyber security incident response exercise developed by the University of Bristol as well as tailored research;
- bespoke products and advice from the Global Cyber Alliance (GCA); and
- stakeholder liaison, promotion, and project management by EDO to optimise implementation of the strategy.

This initiative has the support of your Police, Finance, and Policy and Resources Committees and is now presented to the Court for final approval.

### RECOMMENDATIONS

The Court of Common Council is recommended to:

- approve an uplift of the City of London Police budget for the amount of £870k for 2018/19, and EDO's budget for the amount of £55k;
- approve an increase to the base budget of the City of London Police of £450k and EDO's budget for £55k, for 2019/20 for the initial launch and piloting of Cyber Griffin (over two years), to be drawn from City's Cash; and
- note that, pending the initial success of Cyber Griffin, CoLP and EDO will present a business case to seek long-term funding, to continue to deliver the strategy, beginning in 2020/21.

## MAIN REPORT

### Background

1. Recent cyber-attacks, including *Wannacry* and *NotPetya*, have demonstrated the growing threat of cyber-crime posed to the UK. A recent Government survey showed 43% of UK businesses identified cyber security breaches or attacks in the last 12 months, representing 42% of micro/small businesses and 65% of medium/large businesses.
2. The costs of cyber-crime are significant. In the year ending March 2016, City of London businesses lost over £45 million due to online crime based on National Fraud Intelligence Bureau records. In 2011, the Government estimated cyber-crime undertaken for financial gain cost the UK economy £27 billion every year, although the real impact is likely to be much greater. Although the effect on citizens and Government is considerable, most of the impact is borne by business.
3. The financial services sector is the most vulnerable to cyber-attack. IBM X-Force reported that in 2016, the average financial services client organisation monitored by IBM Security Services experienced 65% more attacks than the average client organisation.
4. These figures reflect the need for proactive, robust cyber defence to protect the City's Financial and Professional Services (FPS) sector, which has been designated as Critical National Infrastructure.
5. The City of London Police are already developing the City of London's cyber resilience and now proposes to build on this extensive expertise to develop and implement a cyber strategy incorporating:
  - A. the Cyber Griffin initiative (see [8] to [11] below);
  - B. a cyber security incident response exercise developed by the University of Bristol as well as tailored research (see [12] below);
  - C. GCA developed technical and subject matter specific products and materials, customised for the FPS sector (see [13] to [14] below); and
  - D. an EDO resource to manage implementation (see [15] to [16] below).
6. Following the two-year pilot, it is anticipated that the strategy, particularly the Cyber Griffin model, will eventually be scaled beyond the Square Mile – across London, the UK and beyond. Ultimately the strategy will grow the City of London's brand as a global leader in cyber innovation, as well as creating opportunities to monetise it directly.
7. The pilot scheme, to be funded for two years, will focus delivery within the Square Mile. Development of the strategy beyond the two-year pilot and beyond the Square Mile will be subject to a business case and funding strategy later in 2019/20.

### A. *Cyber Griffin*

8. Cyber Griffin will be implemented using the Project Griffin delivery model and will aim to prepare the Square Mile's business community for cyber-attacks by focusing on effective defence.

9. Cyber Griffin will offer the following key services for free to businesses in the Square Mile:
- **Base Line Briefing:** monthly open attendance briefings designed to build defender skills in key areas.
  - **Base Line Incident Response:** including table-top exercises developed by Bristol, in which cyber security decision making is evaluated and red flag exercises which examine readiness in real time response conditions and teach key police decision making skills.
  - **Cyber Advisory Group:** an assembly of senior professionals in cyber security, which meets regularly to advise third parties on best practice and appraise new approaches to cyber-threats.
10. Significant demand is anticipated from businesses in the Square Mile for the services offered by Cyber Griffin, as in the City Police's experience:
- cyber security is a leading business concern, but the area is experiencing an extreme shortfall in cyber security personnel;
  - cyber security support is extremely expensive, so access to the free services offered by Cyber Griffin is likely to be popular; and
  - the Cyber Griffin services were developed by consulting with businesses on their priority needs and as a result, some businesses have already signed up to the services to be offered. It is anticipated that, as the initiative is publicised, others are likely to share this interest.
11. By offering its services for free, Cyber Griffin will allow businesses in the Square Mile to:
- to train their staff on key cyber security areas every year;
  - access the latest local and global intelligence while building inter-industry ties and closing intelligence gaps through knowledge pooling; and
  - improve the efficiency and quality of their cyber incident responses.

**B. Bristol University incident response exercise and research**

12. As part of the Base Line Incident Response exercise, Cyber Griffin will offer a premium table-top simulation exercise. Bristol University will be engaged to:
- develop the new table-top exercise, building off its successful 'Decisions and Disruptions' cyber security incident response exercise, to help organisations simulate and ultimately plan for an unfolding attack at board level and within teams; and
  - use insights from its analysis of the exercise to prepare presentation materials to support CoLP briefings, generate practitioner reports, and develop academic articles to inform the wider community about how best to respond to future attacks.

### **C. *Global Cyber Alliance (GCA)***

13. GCA, a not-for-profit entity founded by CoLP, the New York District Attorney and the Centre for Internet Security, is focused on uniting global communities against cyber risk.
14. Under the cyber strategy, GCA will amplify its engagement with the City of London's FPS sector by producing a suite of tailored products and services. These technical and subject matter specific materials will support the frontline training delivered through Cyber Griffin and will include:
  - online best practice guides and other material, which could be co-branded by GCA and the City of London Corporation;
  - cyber workshops and webinars; and
  - a business 'toolkit' targeted at FPS suppliers and customers, including cyber good practice advice and tools to enhance cyber protection.

### **D. *EDO***

15. The Cyber Griffin proposal supports the aim of the Government's National Cyber Security Strategy for 2019 to 2021 to make the UK secure and resilient to cyber threats by equipping citizens and businesses with the knowledge and ability to defend themselves against cyber-attack. EDO can engage with its government contacts to ensure continued alignment on cyber outcomes. EDO can also provide strategic, communications and project management support to help grow the Cyber Griffin brand and promote uptake by businesses through EDO's extensive network of senior professionals.
16. As Cyber Griffin develops as a service and as a brand, EDO can continue to support its growth beyond local service delivery, to wider markets in London, the UK and overseas.

#### **Funding request**

17. The Cyber Griffin programme is currently only supported by one CoLP staff member, which severely limits the reach of the initiative.
18. We believe that funding to engage and train additional officers to roll out Cyber Griffin and enable the purchase of IT equipment is necessary. The funding requested for this element of the strategy is:
  - £400,000 to recruit five Cyber Security Advisers (CSAs) at Constable or Private Constable level to deliver the Cyber Griffin programme;
  - £245,000 for a full suite of training for the five new and one existing CSAs officers; and
  - £20,000 for IT equipment,amounting to a total of £665,000.
19. In addition, the following funding is required:

- One-off funding of £105,000 for Bristol University to provide the table-top exercise and research for Cyber Griffin outlined at [12] above. The City Police will own the intellectual property this generates.
  - One-off funding of £150,000 for the GCA to provide the materials supporting Cyber Griffin outlined at [13] to [14] above.
  - £55,000 to fund the estimated gross salary of a dedicated Policy Advisor in the Economic Development Office.
20. The funding strategy for this Cyber Griffin pilot is to increase the City Police and EDO local risk budgets using City's Cash for the amounts set out above. This budget would be ring-fenced to provide the Cyber Griffin trial.

### **Governance and Reporting**

21. The success of the cyber strategy, for the duration of the pilot program, will be measured by the number of businesses that successfully complete the Cyber Griffin programme. Running at full capacity, for year 1, it is anticipated that up to 100 businesses could be serviced with the Cyber Griffin program, not including those who simply receive the briefing.
22. To ensure that a product of the highest quality is delivered, businesses will be surveyed at the time of completion of the Cyber Griffin programme and again six months after, to measure what difference it has made to their confidence in cyber security and inform future activity. This survey has already been designed and tested.
23. A further business case will be presented to assess the performance of the trial period and seek any further funding required on an ongoing basis, incorporating alternative funding sources and/or monetarisation, during 2019/20 to fund the ongoing operation of Cyber Griffin from 2020/21 (should the pilot be extended into business as usual).

### **Corporate and strategic implications**

24. In addressing the emerging cyber threats facing the City of London, this proposal directly contributes to the achievement of a number of outcomes from the Corporation's Corporate Plan. By building resilience within the City to 'fraud and cybercrime' the proposal primarily maps to Outcome 12 – Our spaces are secure, resilient and well-maintained, under the theme of 'build resilience to natural and man-made threats by strengthening, protecting and adapting our infrastructure, directly and by influencing others'.
25. This proposal also enables the City Corporation to assert national leadership and advise internationally on the fight against cyber-crime, helping to promote the City's world class legal and regulatory framework. This maps to Outcome 6 – We have the world's best legal and regulatory framework and access to global markets.
26. It also ensures the City remains a global hub for FPS innovation by supporting businesses in preparing for technological transformation of the economy and because participation in Cyber Griffin could be a competitive advantage for City firms (Outcome 7 – We are a global hub for innovation in financial and professional

services, commerce and culture). Recent research indicates some firms are already considering how their cyber investment could be a value-add for their customers, either as a market differentiator or the basis for enhanced security-based products and services.

27. More broadly, the proposal will help maintain the competitiveness of the City's FPS offering, when faced with the innovative cyber protection initiatives being launched by its competitors. For example, Mayor de Blasio of New York City recently launched NYC Secure, which includes a free smartphone app which issues warnings when suspicious activity is detected on mobile devices and new protections for the public WiFi network, becoming the first city to provide such services for free (Outcome 9 – We are digitally and physically well-connected and responsive, Outcome 10 – We inspire enterprise, excellence, creativity and collaboration and Outcome 1 – People are safe and feel safe).

### **Conclusion**

28. CoLP seeks to emulate its success with Project Griffin in combatting the cyber threat currently facing the City of London's FPS sector. The proposed strategy, combining the people-focused Cyber Griffin initiative backed by cutting edge table-top exercises and data analysis, and GCA's product offering, represents a holistic approach to deterring and defending against cyber-attacks. By partnering with CoLP, EDO can amplify the positive impacts on the City's cyber environment.
29. The initiatives in the proposed strategy will enable FPS businesses in the Square Mile to build their cyber readiness and resilience through free access to innovation, cyber advice, products, services and skills.
30. Ultimately, this model is designed to be scalable beyond the Square Mile to wider London, the UK and the rest of the world. This will contribute to the creation of a globally significant brand in cyber security, cementing the City's position and enhancing its reputation as a leader in this vital field.

All of which we submit to the judgement of this Honourable Court.

DATED this 24<sup>th</sup> day of May 2018.

SIGNED on behalf of the Committee.

**Doug Barrow, Deputy**  
Chairman, Police Committee