Public Document Pack

Police Committee

Date: **THURSDAY, 24 MAY 2018**

Time: **11.00 am**

Venue: **COMMITTEE ROOMS, 2ND FLOOR, WEST WING, GUILDHALL**

9. **CYBER SECURITY STRATEGY**

Joint report of the Commissioner and the Director of the Built Environment

Item received too late for circulation in conjunction with the Agenda.

John Barradell
Town Clerk and Chief Executive

This page is intentionally left blank

Committees	Dated:
Finance Committee Policy and Resources Committee Resource Allocation Sub-Committee Police Committee	5 June 2018 7 June 2018 5 July 2018 24 May 2018
Subject: Cyber Security Strategy	**Public**
Report of: Commissioner of the City of London Police Director of Economic Development Pol 53-18	**For Decision**
Report authors: Charlie Morrison, Simon Horner	

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) is an active, experienced player in this space, and now seeks to build on its expertise to develop and implement a new initiative, 'Cyber Griffin'. Modelled on its successful 'Project Griffin', it will help the Square Mile's FPS sector better self-protect itself against cyber-attack.

Being cyber secure as a financial services centre, is also essential if we are to maintain our competitive position. Other financial centres are launching initiatives of their own. We must use our own unique assets to create the strongest offer to businesses to help them be more cyber secure.

CoLP and the Economic Development Office (EDO) of the City of London Corporation (Corporation) 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 (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.

Recommendations

1) Policy and Resources Committee to agree in-principle to support and approve the cyber strategy.

2) Finance Committee to agree to uplift the City of London Police budget for the amount of £870k for 2018/19, and EDO's budget for the amount of £55k.

3) Resource Allocation Sub Committee are asked to 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.

4) Police Committee to note the cyber strategy and provide a recommendation to support it to P&R and Finance Committee.

5) 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 Budget.

Links to the Corporate Plan

This proposal primarily maps to Outcome 12 of the Corporate Plan – Our spaces are secure, resilient and well-maintained. In particular, this links to the theme of building resilience to natural and man-made threats ['fraud and cybercrime'] by strengthening, protecting and adapting our infrastructure, directly and by influencing others under the aim of shaping outstanding environments.

This proposal also supports the CoLP Corporate Policing Plan 2018-2023 – Developing a world class digital policing environment, supporting safety by design and leading the delivery of a safe place to live, work and visit.

Main Report

1. Recent cyber-attacks, including Wannacry and NotPetya, 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.[1]

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.[2] 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.[3] 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]

4. These figures reflect the need for proactive, robust cyber defence to protect the City's FPS sector, which has been designated as Critical National Infrastructure.

5. CoLP is 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 (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, CoLP and EDO anticipate 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

---

[1] Department for Digital, Culture, Media & Sport, Ipsos MORI and University of Portsmouth, *Cyber Security Breaches Survey 2018*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701840/CSBS_2018_Infographics_-_General_Findings.pdf (accessed 2 May 2018).

[2] City of London Police, 'Over £45 million lost by businesses in the City of London to online crime in the last year', *City of London Police* [website], 13 June 2016, https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/nfib-news/Pages/Over-45-million-lost-by-businesses-in-the-City-Of-London.aspx, (accessed 2 May 2018).

[3] Cabinet Office and Detica, *The Cost of Cyber Crime: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*, February 2011, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf (accessed 3 May 2018).

[4] Ponemon Institute LLC and Accenture, *2017 Cost of Cyber Crime Study,* October 2017, https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50 (accessed 3 May 2018).

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. Further detail about the Project Griffin initiative is at Annex 1.

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. CoLP expects significant demand from businesses in the Square Mile for the services offered by Cyber Griffin because in CoLP'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 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.

    Further detail about the content, delivery and impact of the Cyber Griffin programme is at Annex 2.

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.

    Further detail on the Bristol offering is at Annex 2.

C. 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.

    Further detail about GCA's offering is at Annex 3.

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

A. Cyber Griffin

17. The Cyber Griffin programme is currently only supported by one CoLP staff member, which severely limits the reach of the initiative.

18. CoLP therefore requests funding to engage and train additional officers to roll out Cyber Griffin and enable the purchase of necessary IT equipment. 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 (further detail on the role of CCTAs is at Annex 2);
    - **£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**.

B. Bristol incident response exercise and research

19. CoLP requests one-off funding of **£105,000**[5] for Bristol to provide the table-top exercise and research for Cyber Griffin outlined at [12] above. CoLP will own the intellectual property this generates.

C. GCA

20. CoLP requests one-off funding of **£150,000** for the GCA to provide the materials supporting Cyber Griffin outlined at [13] to [14] above.

D. EDO resource

21. EDO requests a dedicated Grade E Policy Advisor. The estimated gross salary for this resource is **£55,000**.

E. Total

22. The following table outlines the total funding requested:

Item	Funding request 2018/19 £'000	Funding request 2019/20 £'000
Five CSAs, training and equipment	665	400
Bristol wargame and research	55	50
GCA	150	-
EDO resource (estimated gross salary including pension and national insurance costs)	55	55
Total	**925**	**505**

[5] This estimate is provisional, and subject to finance approval from Bristol.

23. The funding strategy for this Cyber Griffin pilot is to increase the City of London Police's local risk budget and EDO's local risk budget, from City's Cash for the amounts set out in the table above. This budget will be ring-fenced to provide the Cyber Griffin trial.

Governance and Reporting

24. 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, we could service up to 100 businesses with the Cyber Griffin program, not including those who simply receive the briefing.

25. We also want to ensure that we deliver a product of the highest quality, so we will survey those businesses, at the time of completion of the Cyber Griffin programme, and six months after, to measure what difference it has made to their confidence in cyber security. This survey has already been designed and tested.

26. To report against progress for the strategy, we will set up a joint steering group co-chaired by EDO Director and the Police Commissioner, with P&R Chair , Police Committee Chair, and one additional member from each committee.

27. A further business case will then 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

28. 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'.

29. This proposal also enables the 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.

30. 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.[6]

31. 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

32. 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.

33. 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.

34. 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.

Charlie Morrison
Police Sergeant, Cyber Crime Unit
City of London Police
T: +44 (0) 7803 305 436
E: charlie.morrison@cityoflondon.pnn.police.uk

Simon Horner
Head of Policy and Innovation
Economic Development Office
T: 0207 332 3659
E:simon.horner@cityoflondon.gov.uk

[6] TheCityUK and Marsh, *Governing Cyber Risk: a guide for company boards*, 25 April 2018, https://www.thecityuk.com/assets/2018/Reports-PDF/Governing-cyber-risk-report.pdf (accessed 2 May 2018).

Annex 1: Background

1. In 2004, the City of London Police (CoLP) faced sustained terror threats. The City was a high value target and a terrorist incident would have been likely to overwhelm police resources. The situation forced a change in police approach and resulted in the launch of 'Project Griffin' in April 2004. The initiative was designed to help the financial sector better self-protect against terror threats.

2. Essentially, Project Griffin seeks to recruit the community to combat the terror threat. CoLP's highly trained Counter Terrorism Security Advisers (CTSAs) educated City workers on counter terrorism measures, trained security staff working in the City to support CoLP critical incident responses and established lines of communication to make the community CoLP's 'eyes and ears'.

3. Project Griffin's extraordinary success at developing a community-based protection network has resulted in the model being adopted nationally and overseas.

4. The National Counter Terrorism Security Office (NaCTSO) has since developed a complementary programme, 'Project Argus', a multimedia simulation posing questions and dilemmas for participants working in syndicates. Project Argus aims to raise firms' awareness of the terrorist threat and provide practical advice on preventing, handling and recovering from an attack. The initiative highlights the importance of being prepared and having necessary plans in place to help safeguard staff, visitors and assets.

5. The successful implementation of Projects Griffin and Argus relied on the expertise of CTSAs, who are specially trained and tasked by NaCTSO. CTSAs' high level of technical knowledge, has enabled them to deliver effective counter terrorism briefings, advice and presentations to participants and to develop innovative new counter terrorism techniques, such as behaviour detection. CTSAs remain the backbone of CoLP's successful counter terrorism projects.

6. CoLP's experience with Project Griffin suggests a community-based approach will be more effective at promoting cyber resilience in the City of London than current efforts focused on media campaigns and non-technical briefings to audiences on invitation.

Annex 2: Cyber Griffin

A. Overview and impact

1. The Cyber Griffin programme encompasses three operational deliverables – base line briefing, base line incident response and a Cyber Advisory Group – underpinned by a team of specialist Cyber Security Advisers (CSAs) to run these services.

2. Cyber Griffin will be implemented using the Project Griffin delivery model (see Annex 1) and will aim to prepare the Square Mile's business community for cyber-attacks by focusing on effective defence. It will involve the deployment of a comprehensive cyber briefing and training agenda, including a table-top exercise developed by the University of Bristol.

3. While initially restricted to businesses in the Square Mile, CoLP's Project Griffin experience suggests the strategy could, over time, be reproduced and scaled in the wider London area, the UK and ultimately at a global level.

4. Such a cohesive, well-rounded, strategic response to the cyber threat could position the City of London at the forefront of the global response to cyber-terrorism, a first adopter of innovative, cyber defence initiatives and a safer and more attack-ready ecosystem in which to do business.

5. Key stakeholders – including the National Cyber Security Centre (NCSC), the Department for Digital Culture Media and Sport, HM Treasury, Bank of England, cyber security product and service providers, Royal Holloway University London and Queens University Belfast – have expressed support.

6. A failure to develop the City of London's cyber security offering will risk the financial and professional services (FPS) sector remaining more vulnerable to cyber-attacks than it otherwise would be, and unable to respond as effectively in the event of an attack. The City will also languish behind other jurisdictions in growing a cyber ecosystem as part of its financial services offer.

B. Operational deliverables

7. Cyber Griffin will offer a comprehensive cyber training suite to businesses, comprised of:

   - **Base line briefing:** monthly open attendance briefings designed to build defender skills in key areas. The briefings would be based on NCSC's '10 Key Areas of Cyber Security' (2017), applying a modular approach which provides a standard level of education and allows attendees to be certified when they attend a core briefing.
   - **Base line incident response:** an exercise comprising three grades, including an informal consultation in which companies discuss their procedures and readiness with trained officers, table-top exercises in which cyber security decision making is evaluated (see [10] to [13] below), 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, including but not limited to police officers, which meets regularly to advise third parties on best practice and appraise new approaches to cyber-threats, thereby assisting businesses and sharing knowledge.

8. These services will be delivered by CoLP's CSAs. Like Project Griffin's Counter Terrorism Security Advisers, CSAs will be given advanced technical training from a range of sources, to enable them to deliver these services to a high standard.

9. CSA training will be delivered on a continual basis, to ensure CSAs remain at the forefront of the evolving cyber threat environment. This extensive training reflects the importance of CSAs to building the credibility of the programme.

C. Premium training tools, research and analysis

10. As part of the Base Line Incident Response exercise, Cyber Griffin will offer a premium table-top simulation exercise.

11. The University of Bristol (Bristol) will be engaged to:

- develop the new table-top exercise, building off its successful 'Decisions and Disruptions' cyber security incident response execise, 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.

12. Bristol's Cyber Security Group has a long track record of collaborating with law enforcement on cyber security issues. The group combines academic rigour with real world impact. It recently worked with the FALCON unit of the London Metropolitan Police, which adopted the Decisions and Disruptions wargame to educate business leaders on how to protect their companies from cyber-attacks.

13. The Bristol initiative will include:

- engaging Professor Awais Rashid, head of the Bristol Cyber Security Group, to commit 2.5% of his time to the project over 24 months;
- engaging Dr Ben Shreeve to work on the initiative at 40% capacity over 24 months;
- designing, testing and running multiple iterations and conducting rigorous analysis to determine the effectiveness of the new table-top exercise;
- travelling to CoLP for development of the table-top exercise and data collection;
- transcribing recordings from the exercise for subsequent analysis; and
- disseminating results at national and international conferences.

D. Outcomes

14. In the first year of the programme, it is expected Cyber Griffin will have:

- CSAs will have completed their initial specialist training giving them the required skills to deliver Cyber Griffins three operational deliverables, although they will not yet be deemed experts.
- Regular, well attended, cyber threat briefings will be in place and accessible to anyone who works in the Square Mile.
- The first grade of the base line incident response deliverable will be in place, allowing any business in Square Mile to consult with a trained officer to establish the best practice business planning required before an effective cyber incident response can be achieved.
- The second grade of the base line incident response deliverable will be in place, with CSAs regularly running a table-top exercise designed to teach business executives key cyber incident response concepts.
- The third grade of the base line incident response deliverable will be in development. Exercises designed to test business incident response readiness in live time with training on police decision making and logging will have been created.
- The Cyber Advisory Group deliverable will be in place, comprising of experts chosen for their representation of different areas of cyber security and chaired by CoLP. The Group will be available to provide businesses in the Square Mile with reliable, neutral specialist advice.

15. If the programme is supported for four years it is expected CSAs will be leading experts in their field, new incident response exercises (underpinned by Bristol research) will have been created and delivered and the three operational deliverables and the training required to achieve them will be able to be packaged and scaled outside the City of London.

Annex 3: Global Cyber Alliance

1. Global Cyber Alliance (GCA), a not-for-profit entity founded by CoLP, the New York District Attorney and the Center for Internet Security, is focused on uniting global communities against cyber risk across sectors, implementing concrete solutions to mitigate and eradicate systemic cyber risks, and measuring and transparently reporting on the effect of its efforts.

2. GCA now has 206 members, including Barclays, BT and Verizon, across 23 countries. It has provided cyber advice to over 20,000 businesses in the UK alone via its partners.

3. GCA's current offering includes free public access to:

   - **DMARC:** an email system configuration and domain name system (DNS) record which assures users of the sender's authenticity, thereby eliminating email spoofing; and
   - **Quad9:** an internet immune system that stops users from accessing known criminal and malware sites by using DNS to block attacks, and which was recently deployed on New York's public wi-fi network.

4. 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:

   - tailored website content for EDO, CoLP and GCA;
   - online best practice guides and other material, which could be co-branded by GCA and the City of London Corporation;
   - cyber workshops and webinars;
   - regular cyber themed events;
   - media and social media publications;
   - tailored online and offline video assets;
   - a pilot in collaboration with EDO on a Smart Cities 'Internet of Things' offering; and
   - a business 'toolkit' targeted at FPS suppliers and customers, including cyber good practice advice and tools to help businesses enhance their cyber protection.

5. CSAs will use GCA's tailored materials as part of their awareness-raising and training under Cyber Griffin, supported by GCA technical and subject matter experts as required.

6. GCA's cyber-defence products and services complement Cyber Griffin's people-focused, capability-building defence and deterrence activities. Together, they will provide a holistic cyber solution for businesses in the Square Mile.

7. CoLP Commissioner, Ian Dyson QPM, has expressed CoLP's conviction that mass deployment of GCA solutions across the UK and the world will have a significant impact on the reduction of cyber-crime and fraud.