Appendix 1: Original Cyber Griffin Objectives and Outcomes

Objective - Cyber Griffin will offer the following key services for free to businesses in the Square Mile:

- Baseline 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 of new approaches to cyber-threats.

Outcome – From its inception, Cyber Griffin has delivered 232 Baseline Briefings. The original objective was to conduct one public briefing a month; Cyber Griffin now conducts, at minimum, biweekly public briefings. Additionally, this service is also NCSC accredited as are the officers delivering it. This exceeds the initial objective.

Outcome - Cyber Griffin has delivered 63 of the Bristol developed Table Top exercises to date. In addition, Cyber Griffin further developed this exercise into a CoLP variant and won a SANS award for innovation in 2019 for this work. This exercise has also received NCSC accreditation. These results exceed the initial objective.

Outcome - The programme investigated creating a Cyber Advisory Group. It was established over the period of the pilot that this group was not able to offer the value anticipated in the programme's initial objectives. In consultation with the Cyber Security Steering Group, the programme later evolved this service into what is now called the Cyber Capability Assessment. This assessment offers a detailed assessment of an organisation's cyber security maturity level which includes a vulnerability assessment, a comparison of the organisation's maturity gauged against best practice standards as well as a road map for improvement. The initial objective was therefore not met, however, following changes agreed with the Cyber Security Steering Group, this objective was modified and the overall purpose has been met.

Outcome – Beyond the three deliverables detailed in Cyber Griffin's original objectives the programme also developed an Incident Response Training exercise. This is a practical service in which officers teach police command structures and decision making in the context of cyber incident response. This helps to develop improved incident response skills using tried and tested techniques developed in policing. This exceeds the objective set.

Objective - 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 programme, not including those who simply receive the briefing.

Outcome – From its beginning, Cyber Griffin has engaged with over 460 companies and delivered its core services to over 11,000 people. It was identified upon delivery of the programme that companies preferred to select specific services that reflected their current requirements. Whilst some organisations completed all four services within the Cyber Griffin programme, more commonly organisations chose to focus on training large groups of employees via one service delivered repeatedly. The most commonly chosen services were the Baseline Briefing and the Table Top exercise. This objective was partially met.

Objective - 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.

Outcome – An external review conducted by KPMG assessed all the services offered by Cyber Griffin. Included in this review were interviews with a randomly selected group of clients who were able to independently confirm long lasting security improvements facilitated by the work conducted by Cyber Griffin. In addition to the objective above, this report also evaluated and confirmed Cyber Griffin's value for money and listed further developmental opportunities. The change of measure to an external assessment was a choice made by the Cyber Security Steering Group who decided a different range of metrics should be analysed. For these reasons this objective is deemed to have been met.

Outcome – Further positive developments achieved by Cyber Griffin beyond the objectives set include the following: NCSC accreditation of all officers and three out of four services, a digital delivery platform for all services, customer relationship management platforms headed by a Cyber Griffin website, a national webinar series and a home working video series.

Appendix 2: Cyber Security Landscape

1. It is now a largely agreed point that cyber criminality represents a substantial threat to global centres of business such as the City of London. In 2018, the banking industry incurred the highest cyber crime losses of $18.3 million.[1] Moreover, in the coming decade this threat is set to steadily increase.[2] Commonly sighted reasons include:
   - Cyber criminality is hard to attribute and to prosecute.
   - The bar for criminals entering this field is lowering each year as 'off the shelf' hacking tools become increasingly available.
   - This criminality's lucrative nature has driven criminal groups to refine their exploitation of this vein.
   - Cryptocurrency has facilitated the movement of currency on a global scale, in a manner which is challenging to track, and therefore made it possible for any individual with internet access to engage in cyber criminality.

2. There has been significant growth in cyber criminality in the past year; 80.7% of organisations have been affected by a cyber security attack and for the first year 35.7% of organisations experienced 6 or more successful attacks.[3] Analysis have also calculated that collectively security breaches have increased by 67% since 2014.[4]

3. In tandem with this escalation, developed economies are becoming increasingly reliant on technology. The COVID-19 pandemic in March 2020 also triggered an even greater move to digital dependence. This elicited a clear increase of ransomware and phishing campaigns that focused on the human and network security weaknesses in an organisation.

4. In 2020, 62% of organisations were targeted with high-profile ransomware and phishing campaigns, an increase from 56% and 55% in 2018 and 2017 respectively.[5] Phishing campaigns accounted for 22% of all breaches featuring hacking,[6] which corresponded to 1 phishing email for every 4,200 emails sent.[7]

5. Across the landscape, it is well accepted that attack vectors such as ransomware are, 'a big problem that is getting bigger, and *[there is]* a lack of protection from this type of malware in organizations.'[8]

---

[1] Accenture Security, 'The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study' [2019]
[2] NCSC and NCA, 'The Cyber Threat to UK Business' [2017]
[3] North America and Europe Asia, '2020 Cyberthreat Defense Report' 58
[4] Accenture Security, 'The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study' [2019]
[5] North America and Europe Asia, '2020 Cyberthreat Defense Report' 58
[6] Andrew J Nathan and Andrew Scobell, '2020 Data Breach Investigations Report' [2020] Verizon
[7] Symantec, 'Threat Landscape Trends – Q1 2020'
[8] Andrew J Nathan and Andrew Scobell, '2020 Data Breach Investigations Report' [2020] Verizon

6. In response to the rise of cyber criminality, business centres have begun to develop area-based programmes of digital protection. Estonia's Cyber Security Vision 2019-2022[9] sets out ambitious plans to develop a 'digitally secure' and 'cyber literate' society following attacks on its capital Tallinn in 2007. Similarly, Singapore Cyber Security Unity Strategy[10] details a series of monitoring and public engagement programmes designed to achieve the same result.

[9] ETH Zürich Center for Security Studies (CSS), 'Estonia's National Cybersecurity and Cyberdefense Posture - Policy and Organizations'
[10] William Martin, 'Singapore Cyber Security Strategy'.

Appendix 3: Project Griffin - The Predecessor to Cyber Griffin

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

2. Project Griffin sought 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 success at developing a community-based protection network resulted in the model being adopted nationally as well as overseas.

4. The National Counter Terrorism Security Office (NaCTSO) also developed a complementary programme, 'Project Argus', which was a multimedia simulation posing questions and dilemmas for participants working in syndicates. Project Argus aimed to raise an organisation's awareness to a terrorist threat and provide practical advice on preventing, handling and recovering from an attack. The programme highlighted 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, 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 suggested that a community-based approach would be more effective at promoting cyber resilience within the Square Mile than the current efforts which focused on media campaigns and non-technical briefings to audiences on invitation.

Appendix 4: Cyber Griffin

1. Cyber Griffin is a public facing, vendor-neutral police led programme designed to protect the City of London's community from cyber attack. Like its predecessor (Project Griffin) the central idea behind Cyber Griffin is that our best opportunity to tackle cyber criminality lies in our collective defences to it.

2. The programme comprises a small group of technically trained and National Cyber Security Centre (NCSC) accredited officers' who work with the community and offer four core services (figure 1). These core services are outlined on Cyber Griffin's website[11] and also summarised below:

   - **Baseline Briefings:** Non-technical briefings designed to take audiences through today's most prolific digital threats with the aim of teaching the simplest and most functional defences to each. This service is NCSC accredited.

   - **Table Top Exercise:** An interactive exercise used to explore simulated cyber security choices which mimic progressively complex cyber-attacks with the aim of teaching strategy, managing security and decision making. This service is NCSC accredited.

   - **Incident Response Training:** A practical service in which officers teach police command structures and decision making models in the context of cyber incident response. This helps to develop improved cyber incident responses using tried and tested techniques developed in policing. This service is NCSC accredited.

   - **Cyber Capability Assessment:** A detailed assessment of an organisation's cyber security maturity level which includes a vulnerability assessment, a comparison of the organisation's maturity gauged against best practice standards and a road map for improvement.

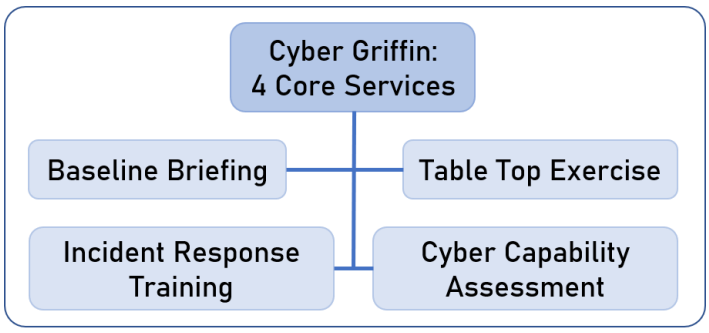

Figure 1: Cyber Griffin's 4 core services

[11] Cyber Griffin, 'Cyber Griffin Website'.

3. In addition to these core deliverables Cyber Griffin have produced a number of other 'peripheral services.' These are bespoke releases in response to a specific development. Two examples include the YouTube home working video series[12] created at the start of the pandemic and the National Police webinar series delivered to support other forces over the same period. The National Police webinar series was also shared *via* YouTube. [13]

4. The programme's current unit comprises one Police Sergeant, five Police/Detective Constable's and one Office Manager. At the time of writing one Police/Detective Constable space is vacant. Figure 2 illustrates the team's current structure (red outline indicating the current vacant position).

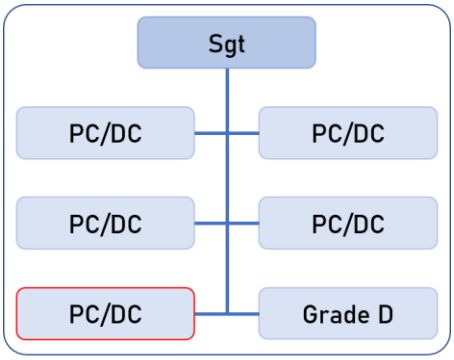

Figure 2: Cyber Griffin structure (as of Feb 2021)

5. Furthermore, as part of its force remit, Cyber Griffin responds to all victim contacts referred to the programme by Action Fraud and through other channels. In this capacity, Cyber Griffin also supports its partner group within the CoLP Cyber Crime Unit, 'the pursue team,' who act as the CoLP's cyber crime investigators. The technical skill sets of the Cyber Griffin officers make them a natural fit for this support role.

[12] Cyber Griffin, 'Cyber Griffin Guides: Home Working' (2020).
[13] Cyber Griffin, 'National Policing Cyber Security Webinars' (2020).

Appendix 5: Cyber Griffin Developmental Projects

A further explanation of the developmental options sighted in point 7 of the proposal:

Cyber Alarm

This is a police led initiative being pioneered as part of Team Cyber UK and designed to keep businesses safe from network level attacks. Cyber Alarm is a software businesses can enable which extracts non-sensitive information from the organisation's firewall and assesses this for digital threats. As more organisations join, Cyber Alarm will grow its ability to detect security risks and inform client organisations. Cyber Alarm has already been successfully piloted in other regions of the country and is continually adding to its core security service to deliver more security benefits. Regional level data storage is now being implemented which allows participating forces to invite and manage organsiations on platforms which the force can manage locally.

Digital Security Coordinators

This is a previously unexplored idea which stems from the current work done by police Security Coordinators (SecCo's). Police SecCo's are trained to assess the security needs and policing requirements of police controlled events. The SecCo's plan informs what police resources will be deployed to the event and the manner in which it will be policed, so as to best maintain safety and security. Should the idea be developed, Digital Security Coordinators (DSecCo's) will support SecCo's by reviewing the digital security of policed events.

Intelligence led Cyber Griffin Services

Currently Cyber Griffin prioritises victims of crime. Beyond this, the programme is made available to the wider public in the Square Mile. Each service is updated based on the latest intelligence however the services themselves are not targeted to groups specifically identified as being at greater risk. Over the next period, Cyber Griffin officers could investigate building this function into the delivery for the programme's core services. The aim would be to maximise impact by delivering services where they are most needed. It should be noted that greater officer resilience would be required to achieve this approach.

Bristol Response Exercise

Throughout the pilot programme, Cyber Griffin have been working with Bristol University to create a new, research based, Incident Response Exercise aimed to directly support cyber incident responders in the financial sector. This exercise is due to be completed in 2021 and will be incorporated into the key services that Cyber Griffin offers. It is of note, that responder skills are one of the strongest aspects policing can deliver to the private sector, it is therefore important that policing develops their offerings within this field as here specifically lies CoLP's opportunity to be world leading.