CoLC/CoLP Cyber Innovation Challenge– Project Plan

Introduction

In 2021 the City of London Corporation (CoLC) and Microsoft partnered to develop an Innovation Challenge bringing together the financial and professional services (FPS) and tech sectors. Cyber security was selected as the theme for the Challenge with a focus on technology to support assessing, continuously monitoring and mitigating risks across the supply chain. The primary aim of the Challenge was to foster collaboration between financial institutions and technology companies. Specifically, the Challenge was designed to:

(i) Cut across silos between traditional sectors and revitalise the ecosystem;
(ii) Challenge organisations to work together on defining and solving a widespread problem statement; and
(iii) Use the opportunities afforded by the Challenge, including the Digital Sandbox platform, to accelerate tech development so that it is market ready.

The Cyber Innovation Challenge involved financial services institutions engaging in weekly meetings with tech companies who were selected for the Challenge via an open application process. During this six-week sprint participants had focused conversations to explore the solutions and how they could be developed to better meet the needs of the FPS sector. The tech companies also attended collaboration sessions to provide them with further insights from across the cyber security eco-system. The Challenge culminated in a final presentation session bringing together all the participants. This provided the technology companies with a chance to present their solutions and explain how they had developed due to participating in the Challenge.

An evaluation of the Challenge has demonstrated positive results. In particular, it confirmed that the Challenge represented a new offering to the market and that levels of engagement from the FPS sector and collaboration between participants to the Challenge were positive. Successful outcomes include pilots that are now being conducted between some of the tech companies and the FPS partners, improvements in the solutions that have been made because of the discussions that took place and partnerships between the tech companies themselves. All those involved in the Challenge who responded to a survey confirmed that they would recommend participating in the programme. All tech companies who completed the survey also confirmed that their involvement in the Challenge accelerated product development.

Cyber Innovation Challenge 2.0

Background

FPS and related sectors remain some of the most targeted sectors for cyber-attacks and these threats are constantly evolving as bad actors develop new methods for advancing cyber threats. As the forms of attack become more innovative, there is an ever-increasing need for more innovative solutions aimed at these markets. There are many who are already working hard to develop products in this area. These range from across the FPS sector, BigTech and other fintech and cybertech specialists. However, there is significant scope to bring better products to the FPS market and wider relevant industry more quickly by supporting collaboration across these sectors. Both CoLC and Microsoft have already indicated an interest in responding to this opportunity by developing an enhanced version of the Cyber Innovation Challenge.

As the national policing lead for cyber, the City of London Police (CoLP) plays a significant role in helping to build a resilient and secure eco-system in which both individuals and businesses across the UK can operate safely. CoLP has a unique insight into the cyber-security challenges that businesses face on a day-to-day basis. CoLP also has information on emerging trends in this area and their potential impact on the business community. This creates an opportunity for CoLC and CoLP to partner on delivering a Cyber Innovation Challenge that will strengthen the UK's cyber security credentials by combining CoLP's strengths as national policing lead for cyber with CoLC's industry and innovation networks and capabilities. A key role of CoLC will be to draw upon its prior experience of running Innovation Challenges of this nature to inform the format and delivery of the Challenge in a way that will be successful. CoLP's primary role will be to provide cyber security expertise and knowledge of both the cyber-security threats and solutions already available in the market. This will be vital to setting the use case, recruiting participants and ensuring that the Challenge is relevant to the FPS, wider relevant industry and tech sector participants that it is aimed at. The primary risk for both parties is advancing a Challenge that will have limited impact on the market and so ensuring that the underlying theme for the Challenge and the format in which it is delivered appeals to the FPS sector is key. Both CoLC and CoLP will have a complementary role to engage their business and broader networks in the Challenge to mitigate this risk.

The Cyber Innovation Challenge advances the CoLC corporate strategy objective to support a thriving economy. It also links to Innovation and Growth's specific business plan objective to ensure that the UK's financial and professional services are at the forefront of tech adoption and innovation. Specifically, the Challenge will support tech to scale by taking innovative solutions that are either at the early stage of development or require support to pivot to the FPS sector to scale. The Challenge supports the City of London Policing Plan priority to protect the UK from economic and cyber crime and builds on its collaboration with industry to improve cyber resilience (National Cyber Resilience Centre Group Ambassador Programme), and share intelligence. This is an objective of both CoLP and CoLPA.

Objectives

The overarching objective for this joint project between CoLP and CoLC is to strengthen the UK's cyber security credentials. In doing so the project should focus on achieving three core aims:

1) Accelerating development of innovative cyber-security solutions that meet FPS and wider industry demand;
2) Supporting cross-sector collaboration and information/data sharing on an emerging and/or key cyber-security challenge (including between industry and policing); and
3) Providing thought leadership on catalysing cyber innovation in the UK.

To achieve these objectives, the Challenge must engage with individuals and organisations from across industry, cyber and tech sectors as well as regulators and government departments operating in the cyber security space. Depending on the use case selected for the challenge there may also be a need to involve data providers, cloud service providers and other areas of law enforcement.

In terms of the project's KPIs, there is scope to draw upon the success criteria that were developed from the previous Microsoft Challenge. In particular, the following are likely to be relevant to the Cyber Innovation Challenge:

1. Market Facing Impact – Proof of accelerated/new product development resulting from the Challenge and the potential for these products to impact industry participants including the FPS market. This will draw upon feedback received from tech participants on the Challenge's role in supporting product development and marketing of their solutions. Any input from industry participants on plans to test and/or integrate any of the solutions coming through the Challenge will also be relevant to demonstrating that this objective has been met.
2. Involvement of key sector representatives including FPS – Numbers and breadth of representation at all stages of the Challenge development and delivery. This is key to ensuring that the Challenge is relevant to the sector and is in the best position to positively impact industry and FPS response to cyber security threats.
3. Collaboration – Evidence of collaboration between different participants in the Challenge. There is a focus on how the industry and tech participants work together (as demonstrated through number of sessions held, feedback provided etc), but it is also important to factor in collaboration with the broader cyber-security eco-system and between tech participants and/or industry/FPS participants themselves. This all has the potential to help improve the understanding of and response to cyber security threats.
4. Thought Leadership - Demonstrating that the Challenge is meeting a need not already being resolved within the market. This can be reflected in the topical and unique focus of the use case underlying the Challenge and/or the format of the Challenge which is not replicated through other groups or forums. This could also be demonstrated by reviewing the number of stakeholders engaged either through the Challenge itself or as part of the lessons learnt and knowledge sharing arising from it.

Project Plan

Fundamental to the successful delivery of the project is agreement between CoLC and CoLP to combine resources and commit to the work required. The following project plan sets out the proposed scope of work, timetable and initial responsibilities to be set between CoLC, CoLP and possible third party partners to the project. As noted above, Microsoft has already confirmed its interest in being involved and there is scope for exploring this and additional partnership roles to support the development and delivery of the Challenge.

	Timeline	**Phase of Work**	**CoLC Role**	**CoLP/CoLPA Role**	**Notes**
1	November 2023	**Confirmation of project plan**	To provide a suggested project plan for CoLP review and input	To provide substantive input into project plan and confirm agreement to committing time and other resource to delivery of the Challenge	Project plan to be signed off by Innovation & Growth SLT and CoLP and presented at ECCC November meeting for approval

	Timeline	Phase of Work	CoLC Role	CoLP/CoLPA Role	Notes
2	December-January 2022	**Initial partnership discussions** – CoLC and CoLP to agree on a list of potential third party partners for the Challenge, clarifying their role and remit eg as experts, funders etc This is likely to be a mixture of 'founding' partners who are involved in the day to day activity of the Challenge and 'supporting' partners who assist with delivery, but are less actively involved. CoLP and CoLC will then work together to approach and recruit partners to the Challenge	To suggest other partners that could support delivery of the Challenge. This will include those that bring specific strengths on technology development, cyber expertise and data. This is likely to include previous Challenge partner Microsoft, but also possibly UK Finance, LORCA and others	To suggest other partners that could support delivery of the Challenge. This should include those organisations with which CoLP / CoLPA has strong ties including the NCSC and who weren't engaged with the previous Challenge, but could provide useful input	It might be sensible to limit the number of 'founding' partners to help align objectives. Microsoft were a valuable partner previously in terms of branding and providing input on cyber security theme, access to relevant industry/FPS contacts. Also worth considering at this early stage broader industry/government partners as were used before who support the Challenge, but are less involved in the day-to-day delivery
3	January-February 2022	**Challenge objectives and evaluation framework agreed** – CoLC and CoLP to agree a set of key objectives for the Challenge and refine with partners to ensure that measures of success are clear and agreed from the outset	To table CoLC objectives expanding on those set out above and taking into account those adopted for the previous Cyber Innovation Challenge	CoLP to ensure that its own objectives are clear and being met as a result of the work to be undertaken across the Challenge	This objectives setting should include agreement of KPIs and how the success of the Challenge will be measured. This includes consideration of how any data will be captured to support the evaluation eg entry/exit surveys from participants
4	January-March 2022	**Challenge use case setting** – it's integral that the Challenge addresses a key cyber-security issue that is being faced by businesses. Initial input on possible topics should be explored by CoLC, CoLP and	To provide initial input on possible use case from stakeholders (via existing contacts/SRM) on top cyber-security challenges being faced by FPS. To organise workshops including proposing attendees	To provide input on possible use case from internal knowledge and intel on emerging cyber-security challenges being faced by relevant sectors. To propose attendees, and jointly agree	In terms of the workshops it would be useful to consider the use cases from three different perspectives: (i) relevance/impact on FPS/relevant industry; (ii) capability for tech solutions to respond to the challenge; and (iii) blockers to

	Timeline	Phase of Work	CoLC Role	CoLP/CoLPA Role	Notes
		other partners before bringing in wider stakeholders from across industry/ FPS and cyber sectors in a series of workshops to discuss and refine an agreed use case	and jointly preparing agenda and leading discussions with CoLP	agenda and leading discussions with CoLC	solutions reaching market eg is there a data issue etc Workshops to include input from both the FPS and cyber/tech sectors
5	March-May 2022	**Challenge timetable development** – a timetable and programme of activity for the Challenge needs to be agreed. This is likely to include 1:1 feedback sessions between industry/FPS/tech participants, wider collaboration/learning sessions, data provision/creation and a public showcase event	To provide information from previous Cyber Innovation Challenge on format adopted and feedback from evaluation report on lessons to be learnt for any future iterations of the programme. Can also seek input from previous participants if helpful	To provide input on how CoLP may be able to support on different aspects of the Challenge eg any relevant data sources that CoLP holds which could be shared as part of supporting the development of tech solutions coming into the challenge	Collaboration between industry/FPS and tech participants is at the core of the Challenge programme. However, depending on the use case selected it would also be good to explore whether there is potential to provide tech participants with access to data or other support that they may need to accelerate development of their solutions
6	April- May 2023	**Industry participant confirmation** – once the use case has been finalised and the Challenge timetable set industry/FPS participants should be approached to take part. Their role will be to work with the tech companies to help them develop their solutions to meet the needs of their respective organisations and broader sectors	To make joint approaches with CoLP to potential industry participants confirming the scope and objectives of the Challenge as well as the time commitment required	To make joint approaches with CoLC to potential industry participants confirming the scope and objectives of the Challenge as well as the time commitment required. This is an opportunity for CoLP to engage with key business contacts eg Cyber Ambassador network	The use case workshops should provide an initial pool of possible industry/FPS participants to approach. There will need to be clarity up front of what time commitment is required and when to ensure that they are able to commit and participate fully

	Timeline	Phase of Work	CoLC Role	CoLP/CoLPA Role	Notes
7	April-May 2023	**Technology participant applications** – to run an application process for technology companies that want to submit solutions into the Challenge. There should be clear eligibility and other criteria against which these will be assessed and a panel constituted to reach a decision on which companies to bring into the Challenge	To provide input on process and potential criteria for assessment from previous Challenge. To draft and publish call for applications and share across networks. To assess applications and inform applicants of outcome	To input on proposed process/criteria for applicants based on CoLP knowledge of cyber security solutions currently in the market. To draft and publish call for applications and share across networks. To assess applications and inform applicants of outcome	Whilst the Digital Sandbox platform was used for the application process previously, it will not be available for this Challenge. A new process for submitting and assessing applications will need to be explored
8	May 2023	**Challenge finalisation** – once all participants are confirmed the programme of activity for the Challenge can be finalised. This will include final scheduling of sessions with all industry/tech participants and any other partners who will be involved in delivery of the Challenge	To confirm final scheduling and features of the Challenge (eg access to data, collaboration sessions etc)	To confirm final scheduling and features of the Challenge (eg access to data, collaboration sessions etc)	With the previous Challenge participants were required to agree to comply with Terms of Engagement. Consideration will need to be given as to whether this is sufficient or more formal Non-Disclosure Agreements are required
9	June-July 2023	**Challenge delivery** – the Challenge will be delivered through a set programme of events. This was previously run as a six-week sprint, but it would be sensible to explore different options for extending the timeframe of the Challenge and	To co-lead delivery of the Challenge including CoLC/CoLP/CoLPA representation at all sessions to guide discussions and provide any additional support required	To co-lead delivery of the Challenge including CoLC/CoLP/CoLPA representation at all sessions to guide discussions and provide any additional support required. To also consider CoLP leading a focused collaboration session	Regular check-ins should also be scheduled with all participants during the Challenge to gather and action feedback wherever possible. Based on previous experience, the Challenge should be timetabled to avoid public and/or school holidays wherever possible

	Timeline	Phase of Work	CoLC Role	CoLP/CoLPA Role	Notes
		building out the programme of activity		on CoLP activity in the cyber security space	
10	September 2023	**Public showcase event –** a public event to demonstrate the work undertaken within the Challenge and the solutions that have been developed as a result	To schedule event, confirm format, recruit participants and send out invites	To support on the delivery of the showcase event and help promote as appropriate	To consider any press release and/or marketing to be carried out through CoLC/CoLP channels to support the event
11	October2023	**Challenge evaluation published –** this report will provide further information about the Challenge as part of the thought leadership to be provided on driving cyber innovation in the UK. It will also demonstrate how the Challenge has met its objectives and/or what lessons can be learnt from its delivery	To draft report jointly with CoLP and arrange for publication and any related press release and marketing through CoLC channels	To review and agree report and promote through CoLP/CoLPA channels	

Resource

The Cyber Innovation Challenge should be viewed by both CoLC and CoLP/CoLPA as a significant project. Time and cost resource needs to be committed by both partners. The likely time resource required from both CoLC and CoLP/CoLPA is around 2/3 days per week from November 2022 – October 2023 increasing up to at least 4 days per week from January 2023. The estimated resource cost is £20,000 and will be covered by CoLC. There is potential for further costs to be incurred in developing and sharing data sets for the Challenge, but this will depend on the use case selected and the support sought by the tech companies participating in the Challenge to develop their solutions.

CoLP/CoLPA will jointly resource the challenge. Det Supt Martin Peters and Det Chief Supt Richard Waight will provide strategic leadership and contribute to the discussions on partners and development of the use case. They will consider involving other experts (such as the CoLP Director of Information Security) in development of the use case. They will be supported by Helen Thurtle who will be the key point of contact for CoLP attending project team meetings and participating in the challenge delivery workshops. The CoLPA project lead will be Oliver Bolton who is responsible for cyber-crime policy and partnerships.

This can be broken down as follows:

Timeline	Phase of Work	Estimated Time Resource	Estimated Cost
November 2022-August 2023	Throughout project	Weekly project team meetings (30/45 min meetings) to share updates, check progress against project plan and milestones and progress any actions or decisions..	N/A
November 2022	Confirmation of project plan	- Review of project plan and meetings to refine the doc (4 hours[1]) - Finalising project plan and presenting for any CoLC/CoLP internal sign-off including joint presentation at the September Economic & Cyber Crime Committee (6 hours)	N/A
December 2022-January 2023	Initial partnership discussions	- Partnership brainstorm (60 min meeting) - CoLC to lead with support from CoLPA: - Preparing partner information pack on Challenge (4hours) - Scheduling/attending meetings with potential partners (12 hours) - Follow up with partners to confirm involvement and role (6 hours)	N/A
January-February 2023	Challenge objectives and evaluation framework agreed	- CoLC to lead with support from CoLPA: - Meetings re-evaluation framework (4 hours) - Gathering input from any other partners (4 hours) - Reviewing and finalising documentation (6 hours)	N/A
January-March 2023	Challenge use case setting	- Gathering input for possible Challenge use case (6 hours) - Initial CoLC/CoLP/CoLPA meetings re Challenge use case (4 hours) - CoLC to lead on organising use case workshops including scheduling, inviting attendees, setting agenda and preparing for workshops (12 hours) - Attending workshops and analysing input received (12 hours) - Final discussions and decisions on use case selection (6 hours)	N/A

[1] This is the likely time commitment required by each of CoLC and CoLP eg 4 hours of CoLP time plus 4 hours of CoLC time.

March-May 2023	Challenge timetable development	- CoLC/CoLPA meetings to develop Challenge timetable and features including 1:1 feedback, collaboration sessions etc (4 hours) - Exploring data asset relevance and availability to be included in support of the Challenge (6 hours) - Preparing overview of Challenge to share with partners (4 hours)	Potential costs to be incurred re making relevant data assets available
April-May 2023	Industry participant confirmation	- CoLC to lead with support from CoLPA: - Preparing list of potential industry participants and preparing documentation to provide an overview of the Challenge, its objectives and the commitment required (8 hours) - Making approaches to industry partners and attending meetings with them (8 hours) - Finalising industry participants (4 hours)	N/A
April-May 2023	Technology participant applications	- CoLC to lead with support from CoLPA: - Agreeing eligibility/assessment criteria for applications (6 hours) - Drafting call for application, application form and publicising across CoLC/CoLP channels and partner networks (10 hours) - Recruiting partners to review and assess applications (4 hours) - Review and assessment of applications (10 hours) - Meetings to discuss application review including compiling comments and finalising list of successful applicants (10 hours) - Informing applicants of outcoming and providing feedback to applicants where requested (6 hours)	N/A
May 2023	Challenge finalisation	- CoLC to lead with support from CoLPA: - Reviewing and finalising Challenge schedule and features (6 hours) - Meetings to finalise Challenge including meetings with all participants for gathering feedback (10 hours) - Circulating final Challenge schedule to all participants and scheduling all sessions across relevant diaries (12 hours)	N/A
June-July 2023	Challenge delivery (based on a 10-week sprint)	- Ensuring CoLC or CoLP representation at each Challenge session to act as facilitator and action any feedback or follow-up (50 hours) - CoLC to lead on regular check-ins with participants to gather feedback (10 hours)	N/A

		- Also providing any additional scheduling or other support to participants and partners during Challenge (20 hours)	
September2023	Public showcase event	- CoLC to lead with support from CoLPA/CoLP: - Confirming format and participants for the event, including briefing sessions for any panel members and/or other presenters (8 hours) - Creation of any video asset/content to support event (10 hours) - Compiling invitee list, sending out invitations and confirming attendees (6 hours) - CoLP and CoLPA attending event and follow-up (4 hours)	£10,000[2]
October 2023	Challenge evaluation conducted and published	- CoLC to lead with support from CoLPA: - To gather any data required for evaluation purposes eg entry/exit surveys, additional feedback sessions from partners and participants (10 hours) - To review and analyse feedback gathered and prepare draft report (10 hours) - External support on report design and finalisation (6 hours) - Finalising and publishing report (4 hours)	£10,000

[2] This represents total estimated cost to be covered by CoLC