Committee(s): Economic & Cyber Crime Committee	**Dated:** 25/06/2024
Subject: Innovation & Growth – Update of Cyber & Economic Crime related activities	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	Driving Economic Growth
Does this proposal require extra revenue and/or capital spending?	No
What is the source of Funding?	NA
Report of: Damian Nussbaum, Executive Director Innovation and Growth	**For information**
Report author: Elly Savill, Senior Policy and Innovation Adviser	

Summary

The core objective of Innovation & Growth (IG) is to strengthen the UK's competitiveness as the world's leading global hub for financial and professional services (FPS). This includes promoting the strengths of the UK's offer and enhancing the UK's position as a leader in FPS technology and innovation.

The following report summarises the activity that has been taking place across IG in relation to cyber and economic crime, as well as cross-team working between IG and the City of London Police (CoLP) since the ECCC last convened in February 2024. The report focuses on next steps for the AI Innovation Challenge.

Links to the Corporate Plan

The activities set out in this report help deliver against the Corporate Plan's outcome to support dynamic economic growth. Specifically, ensuring that the City has the safest, most secure business environment in the world and promoting the UK as a place that is open, innovative, and sustainable.

Main Report

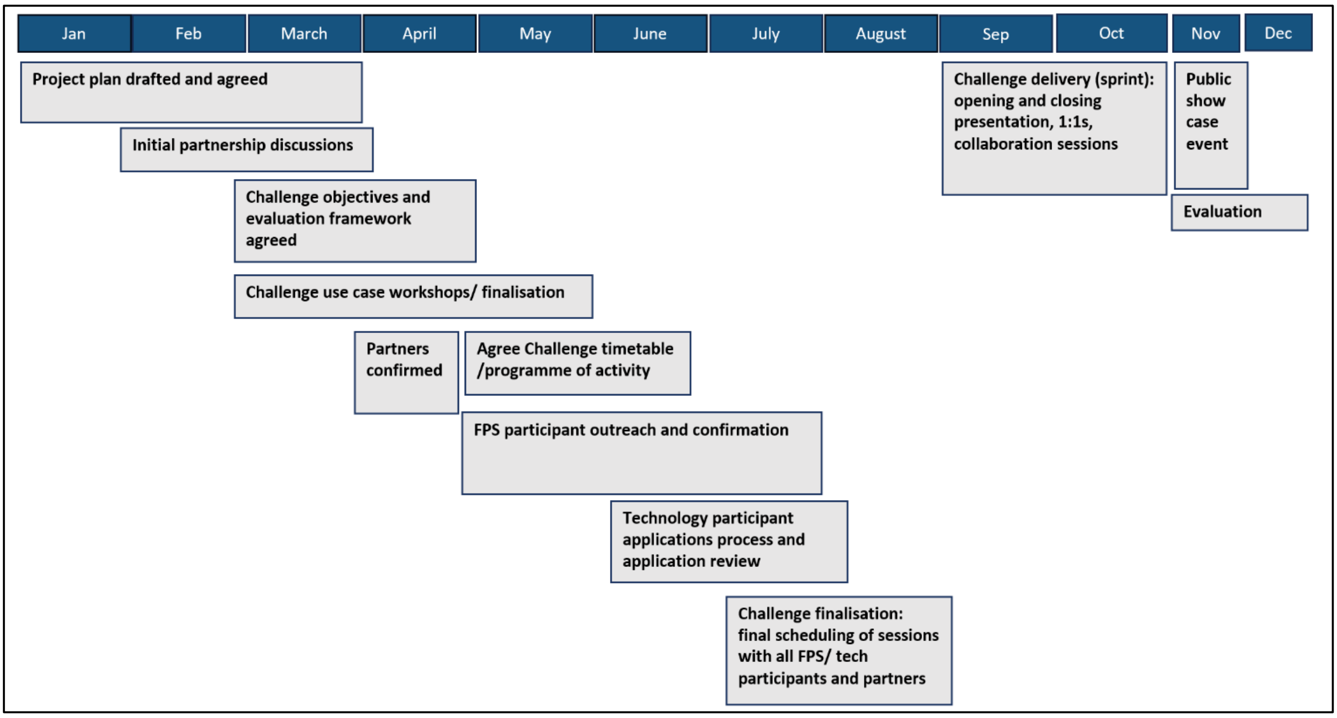
Innovation & Growth activity

AI Innovation Challenge

1. At the last session, IG updated members on plans for an AI Innovation Challenge to be delivered in 2024. The Challenge will support the development of novel AI solutions to tackle a fraud and/or cyber security threats facing FPS. This "use case" will be identified through engagement with key players across the tech and FPS ecosystem.

2. IG has engaged with the Police Authority as well as Challenge Partners Microsoft and the Department of Business and Trade, to discuss the timeline for the Challenge. While the public facing element will run across 6-8 weeks, the

Challenge is a large piece of work running throughout 2024. The following graphic outlines the timeline:



3. A priority for IG is identifying the cyber/fraud threat that the Challenge will work to address. On 20th March, work to identify the use case began with two roundtables welcoming representatives from FPS and tech. Representatives Microsoft and the Police Authority also attended and David Harvey, Director for Cyber Response, KPMG chaired. The roundtables aimed to identify the main cyber security and fraud based threats facing FPS that could be addressed using technology. In addition, the team wanted to understand the tech solutions already available to address these threats and barriers to adoption. These sessions would help to inform the use case that the Challenge would work to address.

4. The FPS roundtable welcomed a diverse group of incumbents, challenger banks, fintechs, legal firms and payments providers. Key findings included:

   a. The use of Machine learning and AI by FPS over 10+ years had shown promise in payments, fraud monitoring and authentication.
   b. Concerns were voiced about how AI could be used to amplify existing threats such as phishing and social engineering. There was a lack of understanding about the potential impact of AI on enabling fraud through fake voice ID and deepfakes.
   c. It was agreed that AI lowered the bar to entry to cybercrime and would likely enable high quality attack vectors with minimal effort.
   d. The impact of AI was viewed as an arms race against threat actors. It was recognised that this would require continual investment in tackling fraud and wider cyber security.

5. The tech sector roundtable welcomed a similarly diverse group of businesses including large household names and startups specialising in AI, cyber security and fraud solutions. Key findings included:
   a. It was highlighted that there were 3 main attack vectors related to AI:
      i. AI Enabled Attacks - such as automated spear-phishing, vulnerability discovery or scanning.
      ii. AI Targeted Attacks - where the attack is against the AI capability, such as data poisoning.
      iii. AI Offensive Attacks - where the AI has agency itself (we have yet to see this but it is a possibility).
   b. Most companies were highlighted as being under-prepared for AI adoption and only 10% were estimated to be resilient to cybercrime. There was a real concern that SMEs were under-reporting and needed to be included in efforts to counter AI attacks.
   c. The continued success of phishing attacks demonstrated that basic cyber hygiene remains an issue.

6. Following the roundtables, a write up was provided by KPMG and Microsoft have since shared additional reflections to help shape the use case. In terms of next steps IG will now undertake targeted 1:1 stakeholder engagement to test ideas and ensure no key themes are missed. This will include representatives from the Police Authority and CoLP. The team will then come together to finalise the use case towards the end of May.

7. In addition to this, a meeting was held with CoLC marketing and media teams to set out key moments for content over the next 9 months. Possible deliverables include talking heads clips with previous participants, infographics and a new web page on Global City.

Corporate & Strategic Implications

8. Strategic implications – This work supports the Corporate Plan outcome to drive dynamic economic growth.

9. Financial implications – All budgets are contained within existing departmental budgets and business planning.

10. Resource implications – All resourcing requirements are scoped as part of departmental business planning.

11. Legal implications – None identified for this paper.

12. Risk implications – None identified for this paper.

13. Equalities implications – The stakeholder work as part of this work is mindful of balancing the needs to have the right stakeholders identified while also supporting the City of London Corporation’s EDI commitments.

14. Climate implications – None identified for this paper.

15. Security implications – None identified for this paper.

Conclusion

16. IG are committed to building on previous iterations of the Innovation Challenge. The team are exploring ways to increase the impact of the project and ensure it is valuable to the FPS and tech ecosystem. IG are also passionate about raising the profile of the AI Innovation Challenge as part of CoLC's commitment to ensuring the UK is a safe and secure place to do business.

Elly Savill
Senior Policy and Innovation Adviser
Innovation & Growth
T: +44 (0) 7500 785073
E: eleanor.savill@cityoflondon.gov.uk