Creating a Cyber Security Directorate:
A new approach for the Corporation of London

January 2018

Executive Summary

▶ Cyber Security is part of the **requirements that all business** must now make provision for – **a new normal for compliance.**

▶ The **cyber crime threat is ever-developing** and the cyber security market place is crowded. This is a new challenge for business and many need assistance.

▶ The Corporation already provides many services that can help businesses meet this challenge but it is fragmented and not visible – we should create a **Cyber Directorate**, leveraging **existing skills and activity** as well as partnering with other London peer group organisations to create a **'single customer view'** on cyber security

The Corporation's Key Objective:

To enable the Square Mile, wider London, and the UK, to access cyber advice, products, services and skills quickly, efficiently and at low cost to make London synonymous with being cyber secure

Now is the time to build a Directorate that works towards our objectives as one City of London

▶ Key Asks:

  ▶ Agree the **strategic objective** on cyber security

  ▶ The **high level aims of the Directorate** as the right means to deliver

  ▶ The **make-up and remit** of the Directorate

  ▶ First **90 days plan**

The Cyber threat is the biggest challenge facing business today

- ▶ This is a relatively **new problem**
  - ▶ New **regulation** is trying to keep up with cyber security compliance.
  - ▶ Businesses must be active in **identifying new and evolving threats**.

- ▶ The **threat can cross borders**. Cyber criminals can operate from anywhere.
- ▶ **Governments and international organisations** are providing services and guidance on cyber – London must show leadership

- ▶ Business is **cautious about sharing data** that may work towards solving cyber security issues.

- ▶ The market place is **difficult for customers to navigate** with providers and services of **varying levels of quality**
- ▶ There is a need to create an **ecosystem** that enables a **functioning, innovative and commercial** cyber security marketplace

- ▶ There is a **disparity in the cyber security capabilities** of large organisations compared to SME's and non-financial services businesses
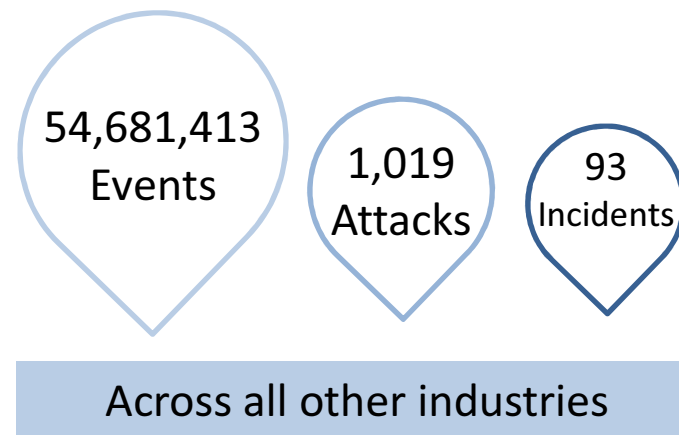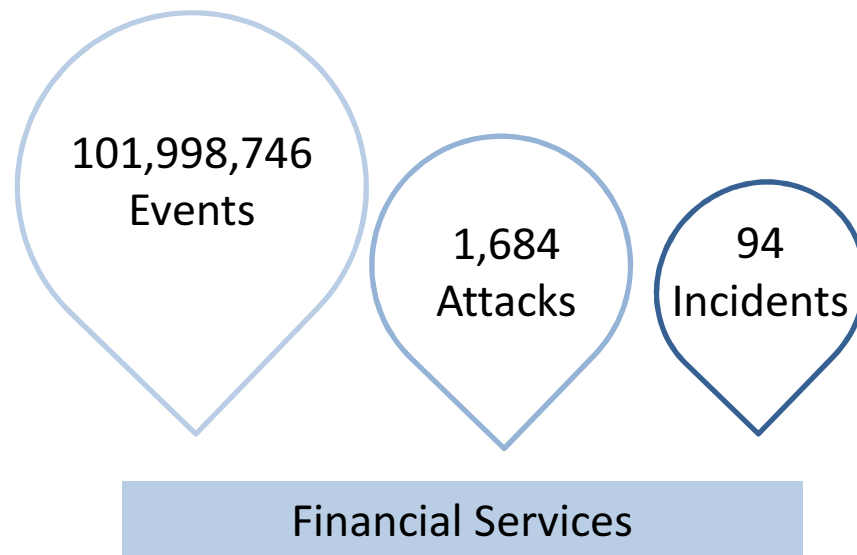 - ▶ Resources
  - ▶ Skills

- ▶ There is a **skills and knowledge gap** in providing cyber security services

Financial services as the cyber criminals' most wanted

In 2016 the financial sector was attacked 65% more frequently than any other sector.

2016 saw an average 29% increase in attacks on financial services organisations—up from 1,310 attacks in 2015 to 1,684 in 2016.

101,998,746 Events

1,684 Attacks

94 Incidents

Financial Services

54,681,413 Events

1,019 Attacks

93 Incidents

Across all other industries

Source: IBM, Security trends in the financial services sector

We must act by leveraging existing Corporation strengths in cyber security…

Key Players
▶ City of London Police
▶ Economic Development Office (EDO)
▶ In-house ICT and information management
▶ Mansion House

CITY OF LONDON POLICE
▶ **National leader on fraud and economic crime**
▶ Sharing data with national authorities
▶ Active participants in industry initiatives like CDA and GCA

Connection and Outreach
▶ The Corporations as a communications platform
▶ Trusted and strong **brand identity**
▶ Connecting business to cyber innovation through our **contacts and events**
▶ Ability to **share best practice** on a global stage

EDO: delivering Skills, Innovation & Enterprise
▶ **Digital skills** development
▶ Connecting sell-side innovators with buy-side incumbents
▶ Inward **investor engagement** and access to finance
▶ Account management – Ensuring UK SME's have **access to export markets**

... combined with wider London's capabilities

Key Players

- ▶ Greater London Authority (GLA)
- ▶ National Cyber Security Centre (NCSC)
- ▶ A financial services industry co-located with a technology cluster
- ▶ Academic Centres of Excellence
- ▶ Bank of England

Regulation & the Courts

- ▶ **Courts,** regulation and policy
- ▶ Stable and up to date legal system
- ▶ Strong insurance sector – growing **cyber insurance** market
- ▶ UK's commitment to adhere to the **General Data Protection Regulation** (GDPR)

Government and Institutional Outreach

- ▶ **National Cyber Security Centre** (NCSC) provide leading guidance
- ▶ Greater London Authority – **London Digital Security Centre**
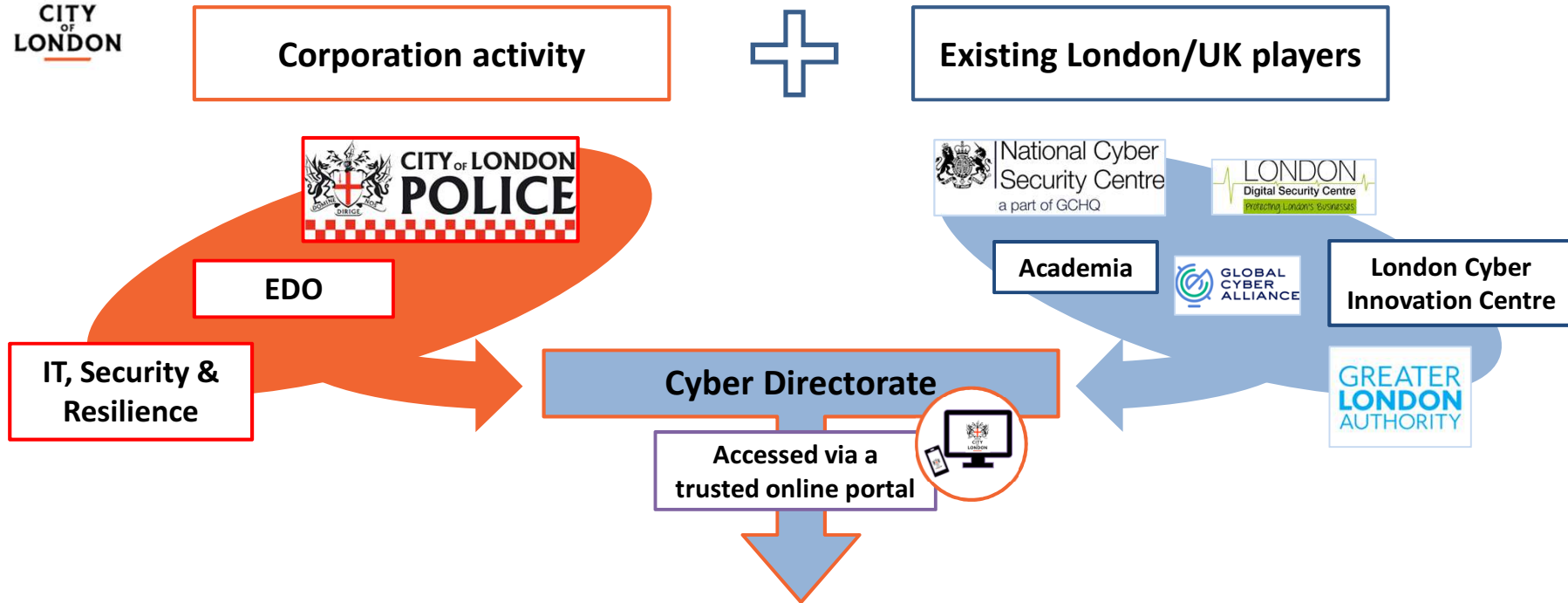- ▶ Growing appetite and regulation for business to **share cyber information**

Skills, Innovation & Enterprise

- ▶ Competitive **existing skills base**
- ▶ Large corporations working on **cyber solutions** e.g. Barclays cyber school
- ▶ Existing environment of **support for SME's and startups**
- ▶ **Academic IP**
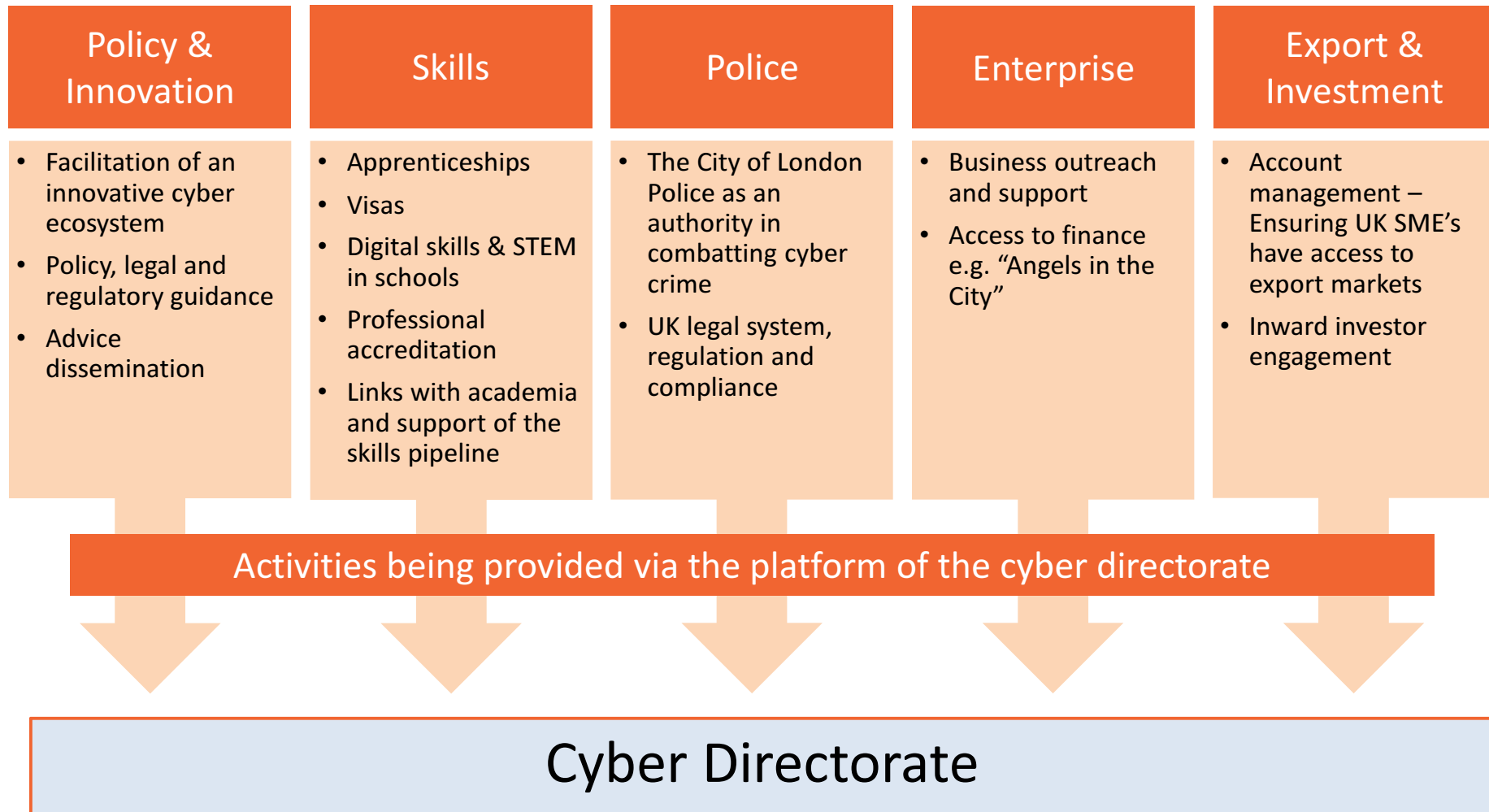- ▶ Forthcoming London Innovation Centre

What the Cyber Directorate could look like:

Corporation activity

Existing London/UK players

CITY OF LONDON POLICE

National Cyber Security Centre a part of GCHQ

LONDON Digital Security Centre Protecting London's Businesses

EDO

Academia

GLOBAL CYBER ALLIANCE

London Cyber Innovation Centre

IT, Security & Resilience

GREATER LONDON AUTHORITY

Cyber Directorate

Accessed via a trusted online portal

The Directorate will provide:	London Boroughs	Public & Third Sector	SMEs	Financial & Professional Services
Advice and Guidance	**Platform for advice** provision to their users	**Dissemination** of Government, COLP and other external advice from partners		Sharing of **threat intelligence**
Products and Services	Providing **access to services** from Police and other approved providers			Access to tailored products and service solutions
Trade & Investment	Develop innovative **London ecosystem**		**Support cyber SMEs to scale up**	**Innovation** and export opportunities

Existing COL activity and engagement will supply the Directorate

Policy & Innovation	Skills	Police	Enterprise	Export & Investment
• Facilitation of an innovative cyber ecosystem • Policy, legal and regulatory guidance • Advice dissemination	• Apprenticeships • Visas • Digital skills & STEM in schools • Professional accreditation • Links with academia and support of the skills pipeline	• The City of London Police as an authority in combatting cyber crime • UK legal system, regulation and compliance	• Business outreach and support • Access to finance e.g. "Angels in the City"	• Account management – Ensuring UK SME's have access to export markets • Inward investor engagement

Activities being provided via the platform of the cyber directorate

Cyber Directorate

The Directorate will package & signpost existing work being carried out by partners

NCSC

- Leading government authority in advice & guidance.
- Apprenticeships and bursaries
- Existing accelerator

GLAs London Digital Security Centre

- Specialise in supporting SMEs
  - Training
  - Guidance
  - Testing capabilities

Academic Centres of Excellence

- Access to solutions and research.
- Continued professional development.
- Space provision and accelerators.

London Cyber Innovation Centre

- Building the cyber innovation ecosystem in London

Activities being delivered via the platform of the cyber directorate

Cyber Directorate

Cyber Directorate leveraging a broad network to provide services to business

Businesses accessing the Cyber Directorate

Skills

Apprenticeship Schemes for non NEC levy payers

- COLP cadets generating cyber participants
- Placements provided within external organisations e.g. GCA
- Corporation connections to industry providing placements

Product

Penetration Testing

- Service provided by the COLP
- Trusted and clear advice to SME's and those with less resource to dedicate to cyber security

Growth

Account Management

- Service provided by the COLP
- Trusted and clear advice to SME's and those with less resource to dedicate to cyber security

Tel Aviv: Effective cyber ecosystem case study

► Key findings from the visit on why Tel Aviv is a leading centre for cyber security:

People	Industry	Academia	Culture
► Compulsory **military service is an important part** of developing the "human capital" in Tel Aviv and powers the tech community.	► International organisations set-up **accelerators and innovation labs in Tel Aviv to access this talent pool**, finding solutions to their problems by working with and supporting start-ups and innovators.	► **Links between academia, government and industry** are a key part of the building and sharing of information and innovation.	► There is an energy in Tel Aviv that is unique in their **approach to entrepreneurship**. They are risk takers but they sit within a supportive community that is not afraid of failure.

Tel Aviv has the right ecosystem but does not have developed internal markets to sell its cyber security solutions to. Therefore it **will always look to export** these solutions

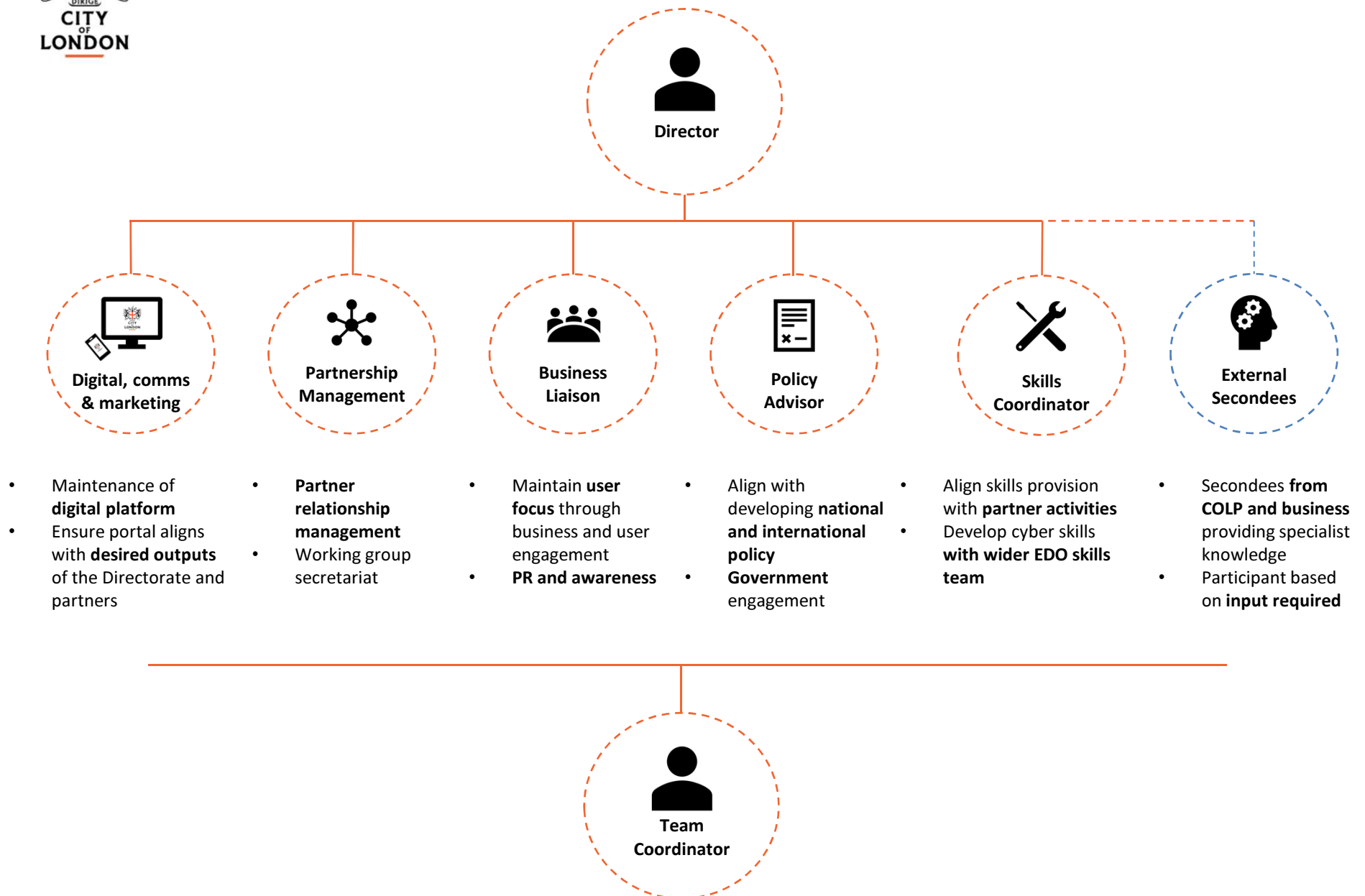**London** can generate cyber security solutions but also has the **right markets and industry** to sell them to

Cyber Directorate: First 90 Days

	Month 1	Month 2	Month 3
CoLC Alignment	• Steering group to set skills/staffing requirements and budget • **Paper to Policy & Resources committee**	• Recruit team • **Key MOUs with Corporation departments** • **Business Plan**	
PARTNER Engagement	• Identify external partners and right contact	• Corporate Affairs /Directorate team to engage and align partners to CoLC objectives	• Formalisation and launch
END USER Engagement	• Develop brand • Partner with account managers to develop **business engagement plan**	• **Develop website** • **Comms/PR plan** • Feedback sessions with end-users	• Finalisation and launch • Work incorporated into Corporations' programme

Key: Products to be designed and delivered are in bold

The team & skills that may be required

City of London

Director

Digital, comms & marketing
- Maintenance of **digital platform**
- Ensure portal aligns with **desired outputs** of the Directorate and partners

Partnership Management
- **Partner relationship management**
- Working group secretariat

Business Liaison
- Maintain **user focus** through business and user engagement
- **PR and awareness**

Policy Advisor
- Align with developing **national and international policy**
- **Government** engagement

Skills Coordinator
- Align skills provision with **partner activities**
- Develop cyber skills **with wider EDO skills team**

External Secondees
- Secondees **from COLP and business** providing specialist knowledge
- Participant based on **input required**

Team Coordinator

To coordinate initial activity the next step is to set up an internal steering group to agree terms of reference, sign off strategy and draw up committee papers

Corporation Steering Group Members

▶ CPR
▶ EDO representative
▶ City of London Police
▶ ICT team
▶ Mansion House
▶ Town Clerks Office

Future London wide engagement

▶ Representatives from the CoLC working group
▶ NCSC
▶ GLA
▶ Winner of the Innovation Centre competition
▶ Academic Centres of Excellence

Now is the time to build a Directorate that works towards our objectives as one City of London

▶ Next Steps

   ▶ **Endorse the concept of the cyber directorate and its basic remit**

   ▶ Form the steering group and immediately progress first meeting

   ▶ Draft terms of reference and necessary committee papers

Annex 1: Tel Aviv Visit. Key themes and resulting tangible actions from the visit to Tel Aviv support the scope and overall aims of the Directorate

► **Skills**
  ► Pilot **apprenticeship programme**, placing a UK apprentice in an Israeli cyber firm.
  ► **"City Cyber Cadets" -** Recruitment of those with a strong existing technical foundation.
  ► Align **digital skills** activities within the Corporation with the development of **cyber security skills.**

► **London cyber innovation ecosystem**
  ► **Forum** between universities in the Square Mile and wider London, government and business to **discuss collaboration on cyber security.**
  ► Meet with universities to **partner in research and encourage the support of start-ups** that have their roots in academia.
  ► Encourage firms to **link to the "applied innovation" that takes place in Tel Aviv** through innovation labs and improving access to the talent and skills pool that is available.
  ► Work with the **London cyber innovation centre** when established and encourage close links with Tel Aviv and Israel.

► **Trade and Investment**
  ► Promote London as a **springboard to global markets for Israeli firms**, aim to support access to finance for those looking to scale up in London.
  ► Use the **Lord Mayors visit** to promote London as an investment destination for Israeli cyber firms.
  ► Explore the **Israeli community in London** and how to develop a campaign to position London as the preferred destination for tech companies.
  ► Understand the **current immigration journey** and if this can be improved for those seeking to arrive in London to work within the cyber/tech sector.