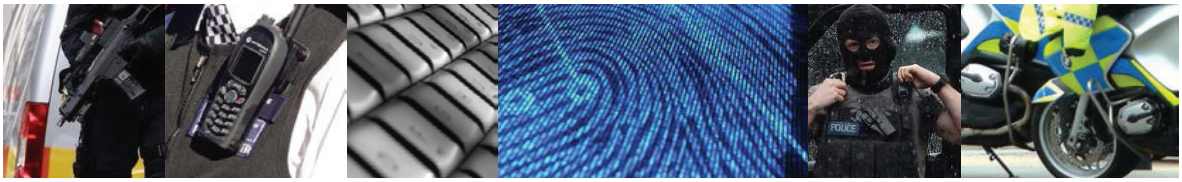
London First

# ‘Intellectual Property Theft’

Breakfast briefing – 17 September 2013

Sponsored and Hosted by Freshfields Bruckhaus Deringer LLP



## INTRODUCTION

A London First Security & Resilience breakfast briefing on Intellectual Property Theft (IPT) was held on 17 September 2013. It was hosted by Freshfields Bruckhause Deringer LLP.

The programme was based on a series of short presentations from:

•Christopher Forsyth, Intellectual Property Partner, Freshfields Bruckhause Deringer LLP.

•Robert Wishart, Detective Superintendent, Head of Operations, City of London Police.

•Dr Darren Brooks, Head of Cyber Risk Advisory Services, BAESystemsDetica.

## A GROWING CONCERN

In 2012 organised crime, fuelled by counterfeiting and piracy, removed $80 billion from the legitimate global economy. According to estimates projected by the International Chamber of Commerce, the global trade in pirated and counterfeit goods will be somewhere in the region of $1.7 trillion by the end of 2014.

## WHAT ARE INTELLECTUAL PROPERTY RIGHTS?

•Intellectual property rights are statutory and legal rights that protect the creative output of individuals and organisations and afford their owners differing degrees of market exclusivity.

•They consist of a mixture of registered and unregistered rights and, while they exist internationally, are enforced nationally.

•The protection of intellectual property falls into four main categories: Copyright, which protects artistic works and software; Trademarks, which protect the unique identifiers that inform consumers of the origin of goods and services; Patents, which protect new and innovative technical developments; and Confidential Information which is not statutory but circumstantial and usually takes the form of contractual agreements.

•Because the legal origins of intellectual property protection remain firmly rooted within the civil courts, criminal organisations have been largely successful in evading the efforts of law enforcement to prosecute them.

•There are, however, three key articles of legislation that allow law enforcement organisations to pursue IPT and infringements in the criminal courts;

-Copyright Designs and Patents Act (1988), Sections 107-112, provide the same protections as civil law but with the extended powers to prosecute those found guilty not only of the unlawful production and distribution of stolen intel lectual property but also those who provide others with the means to do so.

-Trade Marks Act (1994), Sections 82-91, allow for the prosecution of those who are found guilty of trademark infringement which is classified as the use of a similar trademark as another company and/or good. This may cause confu sion among the public as to the provision of that service and/or good.

-Proceeds of Crime Legislation (2002) extends to intellectual property offences and allows for law enforcers to investigate, trace and seize assets from

individuals and organisations, convicted or otherwise, who have been found to profit from the proceeds of crime.

## PIPCU: OPERATIONAL OBJECTIVES AND PRIORITIES

•The Police Intellectual Property Crime Unit (PIPCU) was established in 2013 with a remit to investigate IPT across England and Wales.

•PIPCU is responsible for analysing mass data from public- and private-sector businesses and has strong links to the National Fraud Intelligence Bureau (NFIB) as well as international connections that it is continuing to develop on a bilateral basis.

•Its key operational priorities focus on domain registration, payment service providers, advertising revenues, online market platforms, organised crime groups, and physical supply and distribution.

•PIPCU's main objective is to encourage proactive prevention through altering public perceptions, better collaborative working, improving standards, tackling organised crime, and reducing overall losses.

## THE CYBER DIMENSION

•The threat landscape is characterised by three types of threat: cyber-criminals, who are self-serving and whose key motivation is financial gain; cyber-activists, who are working in aid of a cause and whose key aim is generating publicity; cyber-espionage, which is typically carried out by a nation-state and whose key motivation is to gain a geopolitical or commercial advantage.

•While the risks of cyber-crime remain unique to each individual and organisation, there are a number of counter-measures that prove to be highly effective when managing cyber-threats:

-Prepare: Understand and manage risks and prepare for the risks you wish to mitigate.

-Protect: Protect key information and systems from attack and reduce the impact of attacks.

-Monitor: Monitor systems to detect and frustrate attackers.

-Respond: Manage the consequences of an attack to minimise its impact.