



Environmental Scanning

Economic Crime Directorate

External Issue

27.06.2016



Purpose and Objective

The content of this document is based upon information gathered from open sources by the City of London Police. The purpose of sharing this information is to increase the awareness of issues identified as potential forthcoming economic crime or fraud threats and emerging issues and trends (some may indeed be current).

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared, other than with the agreed readership/handling code, without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998. The cover sheets must not be detached from the report to which they refer.

Protective Marking:	Not Protectively Marked
FOIA Exemption:	No
Suitable for Publication Scheme:	No
Version:	
Storage File Location:	Performance
Purpose:	Environmental Scanning Report
Owner:	SDU
Author:	SDU
Review By:	

Contacts

Questions regarding this document can be sent to NFIBOutputs@cityoflondon.pnn.police.uk

Disclaimer

The information contained within this product is for general information purposes only and does not necessarily represent the views of the City of London Police. The City of London Police produces this product to enhance public knowledge of reported potential forthcoming economic crime or fraud threats and emerging issues and trends. This is a product that is continually under development. While the City of London Police strives to make the information on this product as timely and accurate as possible, we make no claims, promises, or guarantees nor do we give any express or implied warranty about the accuracy, adequacy or completeness of the contents of this product, and expressly disclaim liability for errors and omissions in the contents of this product. Any reliance you place on such information is therefore strictly at your own risk. Efforts will be made to correct errors brought to our attention.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not imply its endorsement, recommendation, or favouring by the City of London Police. The views and opinions expressed herein shall not be used for advertising or product endorsement purposes.

In no event will we be liable for any loss or damage howsoever arising including without limitation, direct, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this product or reliance upon any information contained within it.

With respect to articles linked within this document, The City of London Police do not accept any legal liability or responsibility for accuracy, completeness, or usefulness of any of the information disclosed, or represent that its use would not infringe privately owned rights.

Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.

NOT PROTECTIVELY MARKED

POLITICAL	Page Number
EU Referendum Results – 51.9% Vote To Leave	4
Brexit Implications on National Cyber Security Are Unknown	4
SOCIOLOGICAL/CRIME	
30% Of Councils Suffered At Least One Ransomware Attack In 2015	5
Data Breaches Cost An Average of \$4 million	5
LinkedIn Used by Fraudsters to Harvest Data for Phishing Attacks	5
TECHNOLOGICAL	
Ransomware Provides Live Chat Support To Victims	6
FLocker Malware Spreads To Smart TVs	6
Apple’s New Feature Increases Encryption	6
Google Introduces New Two-Factor Authentication	6
ORGANISATIONAL	
EU Data Centres Are Trusted More Than Non-EU Centres	7
Majority of US Small and Medium Sized Businesses Unprepared For Ransomware	7
Over 50% The World’s Top Sites Could Have Their Emails Spoofed	7
CONSULTATIONS/PUBLICATIONS	
“The Industrialisation of Distributed Ledger Technology in Banking and Financial Services”	8
“Cyber Security: Protection of Personal Data Online”	8
“Are Banks Losing the Innovation Game?”	8

EU Referendum Results – 51.9% Vote To Leave

The UK has voted to leave the European Union after 43 years in a historic referendum. 51.9% voted in favour of leaving the EU. Article 50, the official declaration that a member state wishes to leave the Union, is yet to be triggered.

Linked articles

[The Economist](#)

Brexit Implications on National Cyber Security Are Unknown

Cyber security experts are undecided on the implications Brexit may have on national cyber security. Some experts say that Brexit will have little effect, others stating the opposite. The articles below outline the two sides of the argument.

Linked articles

[Infosecurity Magazine - Cybersecurity still in good hands](#)

[Infosecurity Magazine - Brexit Cybersecurity Ramifications Could be Significant](#)

30% Of Councils Suffered At Least One Ransomware Attack In 2015

According to a recent Freedom of Information request, 30% of UK councils were hit by ransomware in 2015. One council reported suffering 13 separate attacks.

65% of the councils affected said they did not pay a ransom, while 35% did not confirm if they did or didn't.

Linked articles

[SC Magazine UK](#)

Data Breaches Cost An Average of \$4 million

Data breaches now cost an average of \$4 million according to research from IBM and the Ponemon Institute. This is an increase of 29% since 2013. 59% of the cost is associated with cleaning up the incident, such as incident forensics, communications, legal expenditures and regulatory mandates.

Businesses now lose on average \$158 (£112, €141) for every record that is compromised.

Linked articles

[Infosecurity](#)

LinkedIn Used by Fraudsters to Harvest Data for Phishing Attacks

Infosecurity Magazine reports that fraudsters are increasingly looking to sites like LinkedIn to harvest information on employees and their roles within a company, which they can then use to make spear phishing attack.

The security firm, Intel Security, has identified through a poll that over one in five individuals had allowed a stranger to access their details by accepting a connection request. The research also identified that 68.7% admitted they had never questioned whether someone was being honest with their identity on the networking site.

Linked articles

[Infosecurity Magazine](#)

Ransomware Provides Live Chat Support To Victims

The new version of the Jigsaw ransomware provides victims with the opportunity to be guided through the ransom paying process by live chat operators.

Researchers have also identified that once using the live chat feature the victim is able to negotiate a little on the price and is reassured by the extortionist that their files will be decrypted once the ransom is paid.

Linked articles

[Dark Reading](#)

FLocker Malware Spreads To Smart TVs

The FLocker malware, first identified on mobile phones in 2015, has migrated to smart TVs. Once the smart TV is infected by FLocker the screen is locked, a fake LEA notice is displayed and \$200 worth of iTunes gift cards is demanded as payment.

Linked articles

[Tech Central](#)

[The Hacker News](#)

Apple's New Feature Increases Encryption

Apple File System, or APFS, is a new version of the technology that Apple's products use to save and retrieve information. APFS is said to make data retrieving faster and more secure. The technology is the latest move towards further encryption following Apple's standoff with the FBI.

Linked articles

[The Guardian](#)

Google Introduces New Two-Factor Authentication

Two-factor authentication (the method of confirming a user's identity by utilizing a combination of two different components, often a password and a unique code) is an effective method of adding further security to online accounts. It is however often ignored by users as too time costly.

Google has in response made its two-factor authentication process much easier for its users, allowing users to login with a single tap rather than a code. This new method titled "Google Prompt" uses a push notification where users tap on their mobile phone to approve login requests.

Linked articles

[The Hacker News](#)

EU Data Centres Are Trusted More Than Non-EU Centres

Blue Coat Systems have identified that 46% of British, French and German employees trust EU countries to store their data. Comparatively only 18% of those surveyed trust non-EU countries to do the same. The research was gathered from over 3,000 workers in the three countries.

Linked articles

[Infosecurity Magazine](#)

Majority of US Small and Medium Sized Businesses Unprepared For Ransomware

Research undertaken by IDT911 has identified that 75% of US small to medium sized businesses (SMB's) don't have cyber-insurance, or are unsure if their policy includes cyber protection. 65% of SMB owners report that they currently don't and don't plan to budget extra funds for cyber security. 22% of SMB owners say they are unsure how to back up their systems and files and were not aware of the need to do so.

Linked articles

[Infosecurity Magazine](#)

Over 50% The World's Top Sites Could Have Their Emails Spoofed

Researchers at Detectify, a Swedish web security firm have identified that over 50% of the world's top sites suffer from mis-configured email servers; this heightens the risk of spoofed emails being sent using their domain names.

Linked articles

[Threatpost](#)

“The Industrialisation of Distributed Ledger Technology in Banking and Financial Services”

techUK has published ‘The Industrialisation of Distributed Ledger Technology in Banking and Financial Services’, a new paper exploring how to industrialise distributed ledger technology.

Written in partnership with Tata Consultancy Services (TCS), the paper provides a roadmap for financial service institutions looking to implement the technology. The paper also marks the launch of a new techUK Blockchain working group. The new group will explore the potential for this technology in the financial sector and beyond.

Linked articles

[Wired-Gov](#)

“Cyber Security: Protection of Personal Data Online”

The report, published as a result of the inquiry into the 2015 hack of mobile company TalkTalk, recommends sweeping changes to the way the UK deals with cybercrime, looking at both protecting the community and pursuing criminals.

The report suggests changes including:

- Two-year custodial sentences for offenders convicted of cyber offences.
- Fines for businesses that fail to sufficiently defend themselves from cyber-attacks.
- CEO pay that is linked to the strength of the organisation’s cyber defences.

Linked articles

[Infosecurity Magazine](#)

[Cyber Security: Protection of Personal Data Online](#)

“Are Banks Losing the Innovation Game?”

A report published by Neopay has identified that 50% of 18 to 24 year olds do not trust their bank with e-money transactions. This age group is also the most likely to trust a technology company such as Google with an e-money transaction.

Linked articles

[Are Banks Losing the Innovation Game](#)