

Protect Briefing – 2/2/17



GDPR – are you prepared?

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The Information Commissioner's Office (ICO) website has detailed information regarding the implementation of the GDPR rules. The principles are similar to those in the Data Protection Act, with added detail at certain points and a new accountability requirement which requires you to show how you comply with the principles – for example by documenting the decisions you take about a processing activity.

View the GDPR pages on the ICO website [here](#)

How to catch a cyber criminal

This interesting article discusses what it takes to catch a cyber criminal and some of the issues that can arise during a criminal investigation.

Cybercrime investigations have created many new hurdles for prosecuting agencies to overcome and led to many new and innovative techniques being used.

To view the article visit cbronline.com

Post ransomware attack report

As another local council has its IT systems compromised by a ransomware attack please take the time to read the attached report which was produced after a ransomware attack on Lincolnshire County Council in 2016.

The report gives an in depth review of the attack and how it was dealt with along with a number of recommendations to prevent further incidents taking place.

Of note is the need to have a disaster recovery plan in place, continual staff training around IT governance and the importance of working closely with any outsourced IT suppliers to make sure they are providing their contracted services.

To read the full report visit the Lincolnshire County Council [website](#)



The Cyber Essentials scheme provides business' with clarity on good practice within cyber security.

Find out more [here](#).



Ransomware – a billion dollar industry?

This informative article takes an look at the current cybercrime climate and makes a number of noteworthy points regarding businesses response to the threat of cyber attack.

To view the article visit [betanews](https://betanews.com)

Would you report at a cyber attack to Police?

A recent survey by SentinelOne found that only 54% of respondents who had been a victim of ransomware reported the incident to the police.

As law enforcement we need to have an accurate picture of the scale of any problem if we want to effectively tackle it.

If as a business you are unsure as to whether you should report, or the mechanism to do so, feel free to contact us in confidence at the email address shown on the last slide of this briefing

To view the full article visit [infosecurity magazine](https://www.infosecuritymagazine.com)

Take Five scam videos

Take Five is a national campaign that offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud.

They have recently released a number of online videos in an attempt to raise awareness of a number of online and telephone based scams.

Although the videos may appear very simple in their content hundreds of companies a month are falling foul to frauds that are instigated via simple phishing emails or spoofed calls/texts.

To view the videos visit [#scamacademy](https://www.scamacademy.com)



Briefing Dissemination

This document has been given the protective marking of NOT PROTECTIVELY MARKED and may be disseminated outside of law enforcement with no restrictions. Please feel free to circulate it within your business or to other partners.

If you know anyone else who would like to receive this briefing please send us their e-mail address and we will add them to the distribution list. If you no longer wish to receive this bulletin please let us know at the email address below.

Any comments or queries please email the FALCON Cyber Protect team at:

CyberProtect@met.police.uk

