Protect Briefing – 27/2/17

FALCON
FRAUD AND LINKED CRIME ONLINE

Businesses more likely to be targets of cybercrime than any other crime type

According to the National Cyber Crime Unit, part of the National Crime Agency, cybercrime is something that should be on everybody's radar, in any organisation, and all businesses need to understand the massive scale of cybercrime.
A spokesman stated "most businesses will have insurance against things like fire and burglary, which are statistically much less likely to happen than a cyber attack, and yet relatively few have well-developed incident response plans and effective backup and business continuity mechanisms in place,"

To view the full article click here

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

Find out more here.

The 10 biggest cyber attacks

This infographic details the top 10 data breaches and cybercrimes that have been reported. Not only does it highlight the impact on the effected organisations it also emphasises that however large an organisation, and the resources it has available, it is still vulnerable to cyber attack.
With this is mind it is important to reiterate that **all** business are targets for cyber criminals, however small or large they may be.

To view the infographic visit informationsecuritybuzz.com

New cyber security strategy between government and IT suppliers

The government has introduced stringent new responsibilities on IT suppliers in its latest cyber security strategy.
The new strategy sets out dramatic policy changes which will subject companies supplying to the public sector to stricter cyber-related regulations, measure them on a cyber security grading system and actively test the supplier's cyber security measures.
This strategy will have significant impact on the governments IT suppliers and those looking to tender in the future.

To read the full article visit Computerweekly.com

FALCON
FRAUD AND LINKED CRIME ONLINE

The dark web – a guided tour

The increase in cyber attacks has been fuelled by the ease at which criminals can obtain the latest malicious software and advice on how to undertake cyber attacks from online forums for relatively little cost.
This BBC article a explores the underground market places where malware and information is bought and sold and speaks to a cyber security consultant about the evolution of cybercrime for sale and hire.

To view the full article visit bbc.co.uk

What chaos could your ex-employees cause?

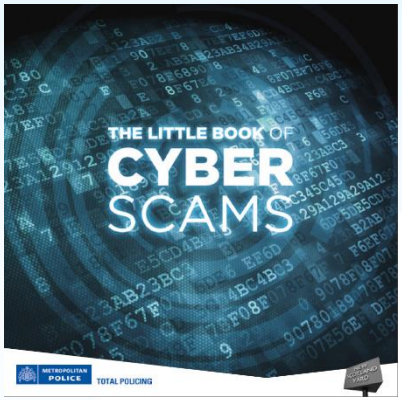
Does your organisation have rigorous policies in place regarding access control for employees leaving their employment? How long does it take for an ex-employee to have their access rights removed?
An article in the Register details how one ex-staff member caused over a million dollars worth of damage to his former employer after gaining entry to their systems after his employment had been terminated..

To read the article visit the Register

Ransomware heads list of most dangerous cyber-attack techniques

Researchers at the SANS Institute have detailed a range of cyber-threats organisations are currently dealing with and ways to become a less inviting attack target.
Speaking at the RSA Security Conference in San Francisco representatives from SANS also identified what they thought were the seven new attack techniques that could be used to compromise computer systems and other internet connected devices.

To read the full article visit eweek.com



METROPOLITAN POLICE
TOTAL POLICING

NEW SCOTLAND YARD

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