

# Compliance & Risk

Volume 6, Issue 3

May/June 2017

## Headlines

- European Parliament rejects money laundering blacklist, p.16
- Facebook fined €110m for false claim in WhatsApp takeover, p.17
- FRC fines PwC £5m for audit misconduct, p.19

## Contents

Data protection codes of conduct hitting the fast lane under GDPR 2

A post-Brexit future for UK financial services in the EU 7

Cybersecurity insurance: transferring the risk 9

News & Views 15

## Massive ransomware attack has global repercussions

A massive ransomware attack on 13 May 2017 which affected 200,000 computer users and closed factories, hospitals and schools is believed to involve malicious software apparently stolen from the US National Security Agency.

Whilst security officials around the world raced to find who was behind the cyber-attack that caused damage across the globe, and authorities braced themselves for additional cyber breaches, the president of Microsoft hit out at the US government.

Brad Smith, Microsoft's

General Counsel, said "The governments of the world should treat this attack as a wake-up call," as he criticised the US government for 'stockpiling cyber weapons'.

The unprecedented attacks, using software called WanaCrypt0r 2.0 or WannaCry, exploits a Windows vulnerability. A patch – a software update that fixes the problem – was released by Microsoft in March 2017, but computers that had not installed the security update remained exposed to risk.

The NSA is believed to have developed the hack-

ing tool that was leaked online in April 2017 and subsequently used to implement the ransomware attack.

Cautioning governments against hoarding cyber weapons, Microsoft's Mr Smith said that "An equivalent scenario with conventional weapons would be the US military having some of its Tomahawk missiles stolen."

In the US, emergency meetings were held during the weekend of the attack to attempt to assess the threat it posed.

[\(Continued on page 15\)](#)

## Weighty fines for Health and Safety offences underline recent trend

Two recent Health and Safety cases in the UK have seen major fines handed down to companies in breach of regulations emphasising the current trend for steep penalties in this area.

An Exeter-based water treatment firm, with an annual turnover in excess of £500 million, was fined £1.8 million after a lone worker drowned at one of its plants.

On 30 December 2013, the individual had been working alone at a Cornwall water treatment facility. The catchment operator was trying to unblock a sand filtration filter, a routine maintenance task, when he slipped and fell through a narrow opening into the 6.5ft-deep water tank.

The company admitted failing to identify the risks posed to lone workers and pleaded guilty to

breaching section 2(1) of the Health and Safety at Work Act 1974.

Although there was no means of escape, the company had put a lone-worker call-in system in place. This emergency feature automatically contacts workers after a period of inactivity. If the worker fails to respond, the system sends an alarm message to an

[\(Continued on page 15\)](#)