THE BUNKER

Part of the CYBERFORT group

DATA SECURITY WHAT WE'VE SEEN AND WHERE IT'S HEADING

2018: THE YEAR OF GDPR

€16.5 MILLON

is the new cap on each fine (or 4% of worldwide turnover), 33 times more than the previous €500k cap.[6]

Sensitive Personal Data and Financial Data: the most common drivers of ICO complaints in the first 5 weeks of GDPR.[6]

Down from 28% in 2017, 13% of global organisations believed they would not be impacted by the data regulations in 2018, despite the introduction of GDPR .[2]

160% INCREASE

in ICO data breach complaints in the period between 25th May and 3rd July.[6]

THE CURRENT DATA SECURITY LANDSCAPE

78%

of businesses surveyed in 2017 planned in an increased IT security spend in 2018.[2]

92%

of malware in 2017 was delivered by email.[3]

In the first half of 2018, less than 3% of breaches have been protected by encryption, so 97% of data lost or stolen is readable.[4]

Since 2013, an average of 6.1 million data records are lost or stolen every day, 257k every hour, 4k every minute, and 71 every second.[4]

HEALTHCARE

is the industry suffering from the highest numbers of breaches, accounting for 27% of incidents in the first half of 2018.[4]

34% of breach incidents in the first half of 2018 were caused by accidental deletion or loss.[4]

Data loss in 2017 was up 400% since 2012.[5]

76.20%

of records stolen or lost in the first half of 2018 have been in the Social Media industry, up from just 0.65% in 2017.[4]

The largest single potential data breach of 2018 involved the exposure of around 340 million records.[9]

46% of people believe that, even after a cyber attack, their organisation's security strategy is unlikely to substantially change.[1]

WHAT'S IN STORE FOR 2019?

A NEW REGULATION

E-Privacy is predicted to take effect in 2019, designed to better protect the privacy of personal data and metadata within electronic communications.

AI systems look to become a growing concern, both as attack targets and as tools employed by cyber criminals. Equally, AI will become increasingly relied on for defence.[9]

Rehab camps for teenagers who are caught carrying out hacking and cyber attacks may be rolled out by the NCA.[7]

5G TO ACCELERATE

with infrastructure estimated to grow from $528 million this year to $26 billion in 2022.[9]

BLOCKCHAIN

is believed to have the potential to disrupt virtually all business models.[1]

Increasing attacks on data in transit are expected, with a focus on personal Wi-Fi routers and poorly secured IoT devices.[9]

A global black market in hacking games appears to be growing.[8]

SOURCES

1. Cyberark Global Advanced Threat Landscape Report
2. 2018 Thales 2018 Data Threat Report
3. Verizon 2018 Breach Investigations Report
4. Breach Level Index
5. Iron Mountain: The Global Cost oOf Data Loss
6. EMW: Data Breach Complaints to ICO More Than Double Year-On-Year After GDPR
7. BBC: Rehab camp aims to put young cyber-crooks on right track
8. BBC: Fortnite teen hackers 'earning thousands of pounds a week'
9. Symantec: Cyber Security Predictions: 2019 and Beyond

Visit **www.thebunker.net** to find out more