☎ +44 113 322 27 90 ✉ info@dcrpartners.co.uk dcrpartners.co.uk

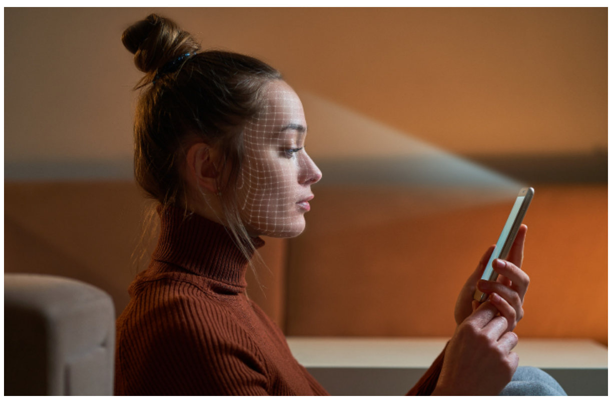
DCR Partners
DIGITAL | CHANGE | RISK

Byte Size Security

YOUR MONTHLY CYBER UPDATE

Issue | 02 | November 2021

Data Privacy



Face Off At Facebook

Facebook plan to decommission their Face Recognition system on the platform and delete over 1 billion facial recognition profiles. This comes amid cries of concern that Facebook had been storing biometric data without consent from users (shock horror). Over a third of Facebook users, some 900 million, had opted in to the Face Recognition feature which had the ability to recognise people's face from 'memories' or suggest tagging based on facial recognition.

> Read more

Robbin' Hood

A cyber attack on Robinhood Markets, who became widely known in 2021 for their association with the Gamestop investing frenzy, has left personal information of customers at risk. A social engineering attack led to a customer service employee giving the attacker access to company systems where they then proceeded to steal data and then demand payment for not releasing the data publicly.

> Read more

Cyber Security

Soaring Energy Bills: Phishing Attacks Not Far Behind

Phishing attacks continue to rise at a staggering rate with the energy industry reporting that they've seen a rise of over 150% since 2020. In addition, with so many people working from home attackers are also targeting VPN credentials in a bid to gain unauthorised access to internal corporate networks. True to form, scammers have latched onto a topic that's worrying many people at the minute, the seemingly neverending rise in energy prices, and are attempting to play on that fear to steal your data / money.

> Read more

Global UnProtect

Thousands of Palo Alto firewalls affected by zero day vulnerability after researchers develop exploit. If used, the exploit could grant access to configuration data and extract credentials to gain control over the firewall giving them visibility of the internal network the firewall should be protecting. Palo swiftly released a patch to plug this terrifying security hole, however this serves as a timely reminder to not take security for granted. Sometimes the security solution itself is the vulnerability.

> Read more

Regulation

Time For Action From The Top

In amongst all the usual goings on at Black Hat Europe in November, Marietje Schaake, former MEP and International Policy Director at Stanford University's Cyber Policy Centre gave a particularly interesting keynote address. Schaake highlighted the weaknesses in current governmental approaches to managing cyber security risks, and highlighted both the inaction towards the internation sale of surveillance / weaponised software and the proliferation of ransomware. Schaake has set out a seven-step action program aimed at helping governments legislate for better cyber security.

> Read more

The Buck Stops With The Board

The Financial Services Information Sharing and Analysis Centre (FS-ISAC) have published their views on the crucial role of Board Risk Committees in understanding an organisation's true cyber risk exposure, and providing informed, proportionate direction to the business on where to prioritise cyber risk management effort. Whilst the average tenure of a CISO is 2.5 years, board members are often present for much longer, giving them a better opportunity to truly understand where risks may lie and track cyber improvements over the long term.

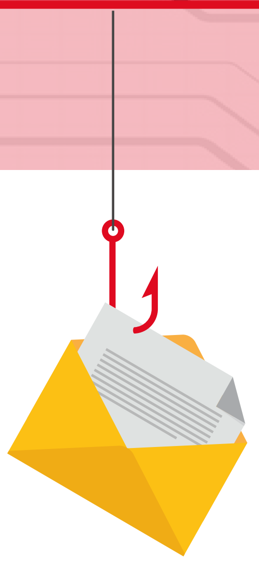
> Read more

Resilience

Unexpected Ransom In Bagging Area

MediaMarkt, an electronic retail company were forced to shutdown IT systems across retail stores in Europe after suffering a ransomware attack in a bid to slow down the spread. Stores across Netherlands and Germany were affected where they were unable to process card payments or print receipts. In a shining example of resilience and business continuity planning, the stores are continuing to operate however employees report being told not to use computers in store, to disconnect tills from the internet and resort to old fashioned operations.

> Read more



One Rule to Block Them All!

In a world overflowing with figures and data, one statistic in particular stood out this month.

Did you know that:

Gmail accounts are used in 91% of all baiting email attacks

With that in mind, is there a case for blocking / filtering / applying additional scrutiny to inbound emails from Gmail?

Would this be too disruptive for your organisation, or in a B2B model should we expect our suppliers to use corporate mail domains?