Cyber_Bytes Issue 67

10 September 2024

Welcome to Cyber_Bytes, our regular round-up of key developments in cyber, tech and evolving risks.

New App - RPCCyber_

As cyber-attacks and follow-on litigation continue to be a board-level issue for organisations worldwide, the RPCCyber_ App provides a one-stop-shop resource for cyber breach assistance and pre-breach preparedness. As well as information about RPC's cyber-related expertise, the app also contains guidance on prevention against common incidents and access to our ongoing cyber market insights.

RPCCyber_ can be downloaded for free from the **Apple Store** or Google Play Store.

The challenges and benefits of the Digital Operational Resilience Act (DORA) compliance

With less than four months until the deadline for organisations within scope to become fully compliant with DORA, RPC's Partner and Head of Cyber & Tech Insurance Richard Breavington has highlighted the challenges and benefits of DORA compliance in a recent interview.

Speaking to InsurTech magazine, Richard highlights the material cost of ensuring compliance with DORA's standards as one of the challenges posed by the new regulation, with the need for implementation of new policies, rules, and processes (such as incident management systems, mandatory threat-led testing, and employee training). Benefits include the harmonisation of previously varied and uneven national regulatory rules, and the establishment of an intelligence sharing mechanism, allowing the exchange of critical information, such as emerging threats and indicators of compromise.

The deadline for entities to become fully compliant with the DORA regulation is 17 January 2025.

Click here to read more from InsurTech magazine.

Cyber-attacks on law firms jumped by 77% over the past year

It has been reported that the number of successful cyber-attacks against UK law firms rose by 77% in the past year to 954, up from 538 the year before. Nearly three quarters of the UK's top 100 law firms have been impacted by cyber-attacks, according to a report by The National Cyber Security Centre.

Law firms often hold information that can potentially be used by threat actors to attempt fraud and other crime, making them an attractive target.

Click here to read more from the Law Gazette.

Law firms have a record of paying ransoms, report claims

A report by technology researcher Comparitech has revealed that law firms targeted by ransomware threat actors have been paid on at least eight known occasions over the past six years. The report identified 138 ransomware attacks on the legal sector, resulting in almost 3 million individual records being compromised.

The largest known ransom demand was $42 million from a New York firm, which was refused. The UK is the second most affected country after the US, with a notable spike in attacks reported in London earlier this year.

Click here to read the full Law Gazette article.

Provisional ICO decision to impose £6m fine on software provider following 2022 ransomware attack that disrupted NHS and social care services

The Information Commissioner's Office (ICO) have decided provisionally to fine Advanced Computer Software Group Ltd (Advanced) £6.09m for failing to implement measures to protect the personal data of 82,946 individuals.

Advanced provides IT and software services to organisations including the NHS and other healthcare providers and acts as a data processor for these organisations.

The fine follows a ransomware attack in August 2022 where hackers accessed Advanced’s health and care systems via a customer account lacking multi-factor authentication. Although no evidence suggests the data was published on the dark web, the attack disrupted NHS services and compromised personal data such as medical records and home entry details for 890 patients.

Click here to read the full ICO article.

NCSC CEO shares insights into securing UK elections in cyber space at major international conference

Felicity Oswald, CEO of the UK's National Cyber Security Centre (NCSC), has emphasised the importance of long-term planning and vigilance in safeguarding the 2024 UK General Election from cyber threats.

Speaking at the Black Hat USA conference, she highlighted how the UK collaborated with partners across government, industry, and international allies to strengthen cyber resilience before polling day.

Despite the traditional use of paper ballots, significant digital infrastructure involved in the electoral process required robust protection against cyber actors. Oswald stressed the need for citizens to trust the democratic process and the integrity of online information. She shared these insights alongside experts from the US and EU, underscoring the global nature of election security challenges. The NCSC also provided updated advice to protect high-risk individuals and organisations involved in the election.

Click here to read the full NCSC article.

Deepfakes: the next frontier in digital deception

Machine learning and artificial intelligence (AI) tools, particularly deepfakes, raise concerns in cybersecurity due to their potential to spread disinformation. Deepfakes can convincingly mimic individuals' voices, making them a powerful tool for cybercriminals as anyone can produce realistic fake content.

This has led to costly scams, such as a fraud where deepfake technology impersonated a CFO and convinced a finance worker to pay $25 million to fraudsters.

Despite advances in AI, the basics of cybersecurity, such as verifying unusual requests and being aware of time-pressured requests, remain crucial. Legislation is emerging to address these threats, with the EU's AI Act categorising AI risks, the UK government's aim to establish AI specific legislation and similar measures being considering in the USA.

Click here to read the full Business Reporter article.