RPC

Key cyber developments

Looking back over 2024

Contents

Introduction

For the cyber market, 2024 brought with it many legislative and regulatory changes, as well as sophisticated cyber-attacks and ground-breaking law enforcement activity. Here we set out a recap of the key developments that took place over the last year.

Richard Breavington
Partner
+44 20 3060 6341
richard.breavington@rpclegal.com

Daniel Guilfoyle
Partner
+44 20 3060 6912
daniel.guilfoyle@rpclegal.com

Rachel Ford
Partner
+44 20 3060 6821
rachel.ford@rpclegal.com

Legislative and regulatory changes

Legislation and regulation continues to develop alongside today's fast-paced technological environment, to ensure adequate protection is in place. We saw the introduction of new legislation and regulation both in the UK and Europe in 2024, some of which is summarised below.

UK

The Cyber Security and Resilience Bill: fortifying the UK's digital defences

The Cyber Security and Resilience Bill (**CSR**) is expected to strengthen the country's digital defences at a time when public services are increasingly targeted by cyber criminals and state actors.

The CSR is expected to (i) update and expand the UK's Network and Information Systems Regulations 2018 (NIS Regulations) so that more sectors are within scope to further protect the UK's national critical infrastructure, (ii) empower regulators, such as Ofgem, to investigate potential vulnerabilities proactively, and (iii) mandate ransomware incident reporting. These are just some examples.

The CSR remains in its early stages. It is expected to be introduced to parliament in 2025.

Data (Use and Access) Bill

The Data (Use and Access) Bill (**DUA**) (formally introduced as the 'Digital Information and Smart Data Bill' in the 2024 King's Speech) reworks some of the measures set out in the former government's Data Protection and Digital Information Bill.

The DUA makes substantial changes to the UK GDPR and offers mechanisms for the government to make subsequent changes (for example, on clarifications as to what should be considered special category data). It does not however substantially change the key notification obligations set out in the UK GDPR in the event of a personal data breach.

The DUA is making its way through the House of Lords and is expected to be in force by Spring 2025.

The Product Security and Telecommunications Infrastructure Act 2022: regulating the Internet of Things

The Product Security and Telecommunications Infrastructure Act 2022 became enforceable on 29 April 2024. The Act aims to enhance the security of consumer connectable products (often referred to as "smart" products) by:

- mandating specific security requirements and standards
- requiring certain entities to investigate and address potential compliance failures (often highlighted by a cyber incident), maintain records, and take corrective actions if necessary
- granting the Office for Product Safety and Standards the power to enforce compliance through various measures, including monetary penalties.

Operational Resilience Rules: the implementation deadline is approaching

The operational resilience rules (**ORR**), published by the FCA, BoE and PRA, created much discussion in 2024.They have an implementation period of 3 years, ending in March 2025.

The ORR apply to certain financial services firms, including banks, building societies, PRA-designated investment firms, and insurers. They include the need for firms to (i) identify business services which if disrupted (including from cyber incidents) could cause significant harm to clients or affect the stability of the financial system, (ii) complete mapping and scenario testing to identify vulnerabilities and implement preventative measures, (iii) report certain incidents to the FCA, BoE or PRA (as applicable), and (iv) have internal and external communication strategies in place to respond to operational disruptions swiftly.

EU

DORA: exploring improvements to cybersecurity in the finance industry

The EU's Digital Operational Resilience Act (**DORA**) required financial services entities and third-party ICT providers operating in the EU to comply with strict new technical requirements and standards to protect against digital threats by 16 January 2025. Those found non-compliant could be fined 1% of their average daily worldwide turnover per day of non-compliance.

DORA also requires compliance with strict notification requirements in the event of certain cyber incidents. For example, during major incidents, companies must submit to the competent authority an initial notification within four hours from the time the incident is deemed to be a major one and, in any event, within 24 hours of awareness. 72 hours after the notification, companies must also provide an incident update and within one month, a final incident report must be produced which contains analysis on resolution, impact, and root cause.

You can subscribe to RPC's DORA Watch for further updates here.

NIS2 Directive: a directive focused on cyber security

The Network and Security Directive 2 (**NIS2**) is an EU directive that entered into force on 16 January 2023, with an implementation date of 17 October 2024 for all EU Member States.

NIS2 updates minimum cyber security standards across the EU for certain, specific sectors and businesses. The directive also introduces mandatory incident reporting whereby initial notifications must be made within the first 24 hours of detection, with detailed follow-up reports being made as the threat is addressed.

Many of the member states across Europe are yet to implement the directive into national law.

For a more detailed analysis, please refer to our article on the NIS2 Directive here.

Cyber Resilience Act: a focus on products with digital elements

On 10 December 2024, the EU's Cyber Resilience Act (**CRA**) came into force, but its applicability is spread across dates ranging from June 2026 to December 2027.

The CRA establishes cybersecurity standards and obligations to notify authorities of severe incidents arising from 'products with digital elements' (**PDEs**), which include the Internet of Things (**IOTs**), computer components and even software. Failure to comply with the CRA obligations can result in a fine of up to EUR 15 million or up to 2.5% of worldwide turnover. Non-compliant products can also be banned, withdrawn or recalled from the EU.

For a more detailed analysis on the CRA, please see our article here.

EU AI Act

The EU AI Act (**AIA**) provides a new risk-based framework for AI systems and for the operators that supply and use those systems in the EU. It came into force in August 2024 and will be implemented over a three-year period with most of its provisions applying from August 2026.

The requirements vary depending on the type of AI system and the purposes for which it will be used. There are detailed requirements for general-purpose AI (**GPAI**) and 'high-risk' uses of AI, while low risk uses will be largely unregulated. In scope AI systems which are high-risk must achieve appropriate levels of cybersecurity standards.

For more detailed analysis on the EU AI Act, please see our article here and for further information on AI, please see our AI Guide.

Cyber incidents

Here we set out a selection of some of the more significant publicised cyber incidents that have taken place in 2024. At RPC, we have dealt with thousands of cyber-incidents over the years and continue to engage with our clients daily on cyber response instructions.

We've created a quick reference guide outlining commonly recurring notification obligations in the event of a cyber incident – for specific legal advice, please get in touch at cyberuk@rpclegal.com.

March 2024: Scottish NHS Trust Dumfries and Galloway

In February 2024, NHS Dumfries and Galloway suffered a cyberattack in which a ransomware group exfiltrated a large amount of patient and staff data, including personal and sensitive medical data, such as x-rays, test results, correspondence between medical professionals and patients, and complaints letters. The threat actor threatened to release the data unless their demands were met, and subsequently published over 3TB of data on the dark web in May 2024.

The attack is one of the more serious in Scotland to date and triggered an investigation by Police Scotland, the NCA, the National Cyber Security Centre and GCHQ, although the police said that a criminal justice outcome is unlikely. The same ransomware group were also responsible for attacks on other public authorities, including a children's hospital in Liverpool, Leicester City Council, the Ministry of Defence, the United Nations and the British Library.

July 2024: CrowdStrike

American cybersecurity company, CrowdStrike, made headlines in July 2024 due to a faulty software update it deployed to its Falcon platform which caused one of the largest IT outages in history.

The update disrupted various sectors worldwide, including air travel, banking, and healthcare, causing impact to millions of computers. CrowdStrike's Falcon platform integrates into Microsoft Windows and is updated regularly; however, a logic flaw in the sensor configuration update caused it to crash, taking Microsoft Windows with it.

CrowdStrike were able to deploy a fix within 79 minutes; however, implementing the fix was labour intensive for some recipients and the disruption caused was widespread, taking much longer to remedy. It has been estimated that the outage will cost U.S. Fortune 500 companies $5.4 billion and cost the UK economy up to £2.3 billion.

The mistake led to CrowdStrike apologising in formal testimony to the US House of Representatives and facing a civil claim by shareholders for allegedly making false or misleading statements about the adequacy of its software testing procedures. In addition, Delta Air Lines brought a civil claim against CrowdStrike in October 2024 alleging negligence resulting in an estimated loss of US$500m; CrowdStrike denies the claim and is counterclaiming.

May 2024: Billericay School

Schools can be a prime target for cyber-attacks. The Cyber Security Breaches Survey 2024, published by the Department for Science, Innovation and Technology,

found that 71% of secondary and 52% of primary schools reported a breach or attack in the past year.

The Billericay School, Essex, reported a "significant cyber/malware attack" during the half term holiday in a letter to parents and carers on 31 May 2024. The school had to close in order for the issues to be resolved.

In a follow up letter, the school informed parents and carers the cyber criminals may have obtained students' information such as names, addresses, basic medical information as well as dates of birth and contact details for parents and carers.

July 2024: the Paris Olympic events

In the lead up to the Paris Olympic games, France was on high alert for cyber-attacks and with good reason. Whilst a reported 1.8 million people attended the games with their digital tickets and 204 countries participated, the French cybersecurity body, Agence Nationale de la Sécurité des Systèmes d'Information (**Anssi**) reported over 140 cyber-attacks during the games in July 2024. 119 of those attacks were reportedly low-impact and just over 20 were considered as successful malicious attacks. Government entities were the primary targets with critical sporting, transport and communications infrastructure all in the sights of threat actors.

August 2024: Locata

Locata, a housing software provider for councils across the UK, was the subject of a cyberattack in August 2024. The attack initially impacted one council in Greater Manchester, but quickly spread to at least two more councils.

Bolton, Salford and Manchester Councils had to suspend their housing websites as a result of the incident. In addition, thousands of users received a phishing email, which contained a link to 'activate your tenancy options' which would have resulted in them giving away their personal data.

The BBC reported that Salford City Council's housing search register was still down weeks later, leaving people unable to get a home as a result of not being able to access the website.

September 2024: Transport for London

In September 2024, Transport for London (**TFL**) fell victim to a cyber-attack which affected its key IT infrastructure.

TFL confirmed that "certain customer data was accessed...This included names and contact details for some customers along with email addresses and home addresses where provided". Oyster card refund data had also been accessed, and 5,000 customers were said to be impacted by the breach. The incident also exposed 30,000 employees' passwords.

On 12 September 2024, the Financial Times reported that a 17 year old teenager was initially arrested in connection with the attack but had then been released. On 28 September 2024, the BBC reported that TFL had indicated the attack was sophisticated in nature and unfortunately ongoing.

As a result of the cyber incident, live bus and train data was limited on some travel apps and certain online services were also affected. The Financial Times also reported that the 47 stations that were going to have contactless payment readers installed by 22 September could no longer achieve this planned delivery date due to the attack.

November 2024: Microlise

UK fleet management and supply chain company Microlise was targeted on 31 October 2024 by a new ransomware gang. This caused the company's tracking system to go down and left British prison vans without functioning tracking systems or panic alarms. Microlise also provides technology to 88% of UK grocery retailers' fleets and the attack caused widespread disruption, affecting clients such as DHL and Serco.

The threat actor claimed to have stolen 1.2TB of data and threatened to publish it if their ransom demands were not met. This threat appears not to have materialised. While Microlise confirmed that no customer systems data was compromised, some employee data was accessed and corporate data from its headquarters was exfiltrated.

Activity from regulators

In 2024 we continued to see regulators assess and mandate the ever-evolving cyber security landscape, offering guidance, publishing reports, and carrying out enforcement action to ensure robust protection against emerging threats and risks.

Sanctions and ransomware guidance from OFSI

In May 2024, the Office of Financial Sanctions Implementation (**OFSI**) issued further guidance on financial sanctions related to ransomware. The government advises against making such payments. Key points of the guidance are:

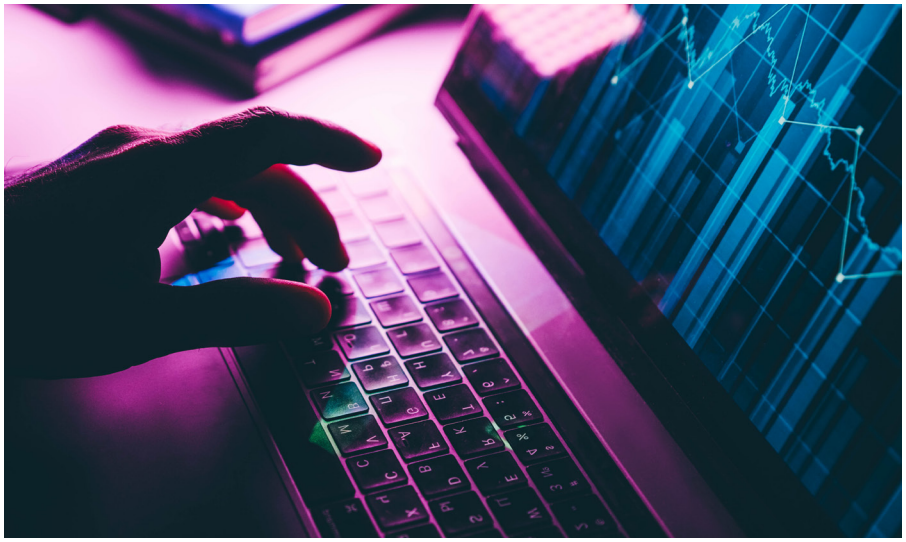
- victims of ransomware attacks should report incidents promptly through a designated portal to receive support and guidance. The National Cyber Security Centre can also provide advice on measures to enhance cyber resilience and reduce the risk of successful attacks.
- businesses should carry out sufficient due-diligence prior to any payments being made, and consider whether sanctions might affect their transactions.
- voluntary disclosure of financial sanctions breaches, as well as general co-operation with law enforcement and the authorities in advance, will generally be a mitigating factor when OFSI assesses the case and any potential enforcement action.
- legal advice should be obtained if unsure about compliance.

OFSI may refer breaches of financial sanctions to the NCA for further investigation where appropriate. If there was public interest to pursue criminal prosecution for a company's breach of sanctions in the event of a ransomware payment, the ultimate decision maker would be the Crown Prosecution Service.

Click here to read the guidance.

Data processor faces ICO action

UK based IT company, Advanced Computer Software Group Limited (**Advanced**), whose business includes hosting activities, received a fine of just over £6m from the ICO following a cyber incident.



The ICO found that Advanced failed to put in place appropriate security measures to protect data (including some sensitive information) of nearly 83,000 people.

Advanced acts as a data processor and its customers include the NHS and other healthcare providers.

Whilst this is a provisional decision, and the ICO awaits receipt of representations from Advanced, it is a first for the ICO – taking action against a data processor for breaching UK data protection laws.

ICO reprimands Electoral Commission

On 30 July 2024, the ICO reprimanded the Electoral Commission over cybersecurity failings relating to an attack in August 2021.

Hackers entered the Electoral Commission's servers and exploited a known flaw in the software. This resulted in personal data, including names and addresses of approximately 40 million voters being exposed to hackers for over a year until the problem was found.

In their report, the ICO state that the Electoral Commission did not have appropriate security measures in place to protect the personal information it held and did not keep its servers up to date with the latest security patches issued. The ICO also found that the Commission did not have sufficient password policies in place at the time of the attack, with a large number of its staff still using default passwords.

Activity from law enforcement

Last year saw some major activity and breakthroughs for law enforcement in the cyber space. Cross-nation collaboration has enabled authorities to bring down/sanction some significant cyber criminals.

Operation Cronos: international task force takes down ransomware titan LockBit

LockBit is a cybercriminal group specialising in ransomware as a service. They write ransomware software which they then offer to affiliates for a fee. This enables a wider class of individuals to carry out ransomware attacks as the affiliates do not necessarily need the same technical skills as the coders.

LockBit was prolific in its criminal endeavours, described by the NCA as once the world's most harmful cyber-crime group. In 2024 a taskforce of law enforcement agencies from 11 countries together with Europol and Eurojust seized control of the darknet websites belonging to the gang, arrested four individuals and named two more. The NCA said that it had "taken control of their infrastructure, seized their source code, and obtained keys that will help victims decrypt their systems" and that this "compromised the entire criminal enterprise". A decryptor for LockBit 3.0 was made available using the seized keys and released to be downloaded for free from No More Ransom.org.

After the takedown, law enforcement officials posted information about the group and its leader, including that it had 188 affiliates and profits from ransom activities of 2,200 BTC or US$112 million.

Operation Endgame: end of the franchise for group of droppers

A dropper (or loader) is a type of malicious software used to deliver and install other malware onto a victim's computer system. It is essentially a digital envelope for malicious software such as trojans, ransomware or keyloggers. Droppers, including those called IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee and Trickbot were the target of an international law enforcement operation carried out in May 2024. Operation Endgame was a collaboration between 12 countries, as well as Europol and Eurojust.

In the first coordinated international operation of its kind, 4 arrests were made, 16 locations were searched, more than 100 servers were taken down or disrupted and over 2,000 domains were seized between 27 and 29 May 2024. Following the action day, eight individuals were added to Europe's Most Wanted list. Operation Endgame is ongoing.

Sanctions for 16 Evil Corp members

Many have heard of the cybercriminal group, Evil Corp. In fact, in October 2024, the National Crime Agency published a document entitled "Evil Corp: behind the Screens" for high level overview of what it calls "the most pervasive cybercrime group to ever have operated". The NCA confirms the group has been operational for at least ten years and has extorted at least $300m from victims worldwide.

Given its notoriety and large scale cyberattacks, it has garnered the attention of the NCA and other international authorities for many years. In 2024, the NCA announced that "Sixteen individuals who were part of Evil Corp, once believed to be the most significant cybercrime threat in the world, have been sanctioned in the UK".

Australia and the US have also imposed sanctions and the NCA has reported that an indictment against a key member of the group has been unsealed.

LabHost criminal website results in arrests of 37 individuals

April 2024 saw a combined investigation of authorities from 19 countries successfully take down the website LabHost and arrest 37 individuals connected to it.

The website was designed to allow users to set up phishing websites, for a monthly fee, either by creating new sites or allowing the use of existing ones.

Europol announced this takedown was due to an "international investigation" that was led by the Metropolitan police "with the support of Europol's European Cybercrime Centre (**EC3**) and the Joint Cybercrime Action Taskforce (**J-Cat**) hosted at its headquarters".

The BBC also reported that personalised messages were going to be sent to the email addresses of those that had been paying for the LabHost services, informing them the police are aware of them and the service they were paying for.

Conclusion

The year of 2024 was certainly an active one for the cyber market, across all fronts.

Advancements were made on both sides of the coin; we saw positive and significant law enforcement activity and legislative change, but we also saw some of the most significant cyber attacks to date.

None of this appears to be slowing down in 2025; government progress with legislation aimed at providing protections against the fast-paced technological environment, whilst threat actors continue to develop sophisticated and ever changing tactics.

As this continues to be a board-level issue for organisations worldwide, the RPC Cyber App provides a helpful resource. 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. RPC Cyber can be downloaded for free from the Apple Store or Google Play Store.

Contacts

Richard Breavington
Partner
+44 20 3060 6341
richard.breavington@rpclegal.com

Ian Dinning
Senior Associate
+44 7843 525064
ian.dinning@rpclegal.com

Lauren Kerr
Associate
+44 20 3060 6775
lauren.kerr@rpclegal.com

Daniel Guilfoyle
Partner
+44 20 3060 6912
daniel.guilfoyle@rpclegal.com

Christopher Ashton
Senior Associate
+44 7731 923163
christopher.ashton@rpclegal.com

Elizabeth Zang
Associate
+44 7851 243222
elizabeth.zang@rpclegal.com

Rachel Ford
Partner
+44 20 3060 6821
rachel.ford@rpclegal.com

Bethan Griffiths
Senior Associate
+44 7734 000160
bethan.griffiths@rpclegal.com

Emanuele Santella
Associate
+44 7549 020663
emanuele.santella@rpclegal.com

rpclegal.com