

# NEWS BRIEF

Provided by: The Risk Hub Ltd

## Cyber-attacks Continue Across UK and Europe

On 6th September, Intercontinental Hotels Group (IHG)—the owner of Holiday Inn—confirmed it had fallen victim to a cyber-attack. In a statement, IHG said it was investigating “unauthorised access” to a number of technology systems.

The acknowledgement comes two days after the UK-based company’s booking channels were disrupted, preventing many customers from booking accommodation online. Furthermore, this event comes just weeks after a Holiday Inn in Istanbul was breached by the ransomware LockBit, resulting in the release of stolen company data.

### Other Notable Cyber-attacks

Cyber-attacks on governments, companies and other organisations have multiplied recently. For instance, transport company Go-Ahead—which runs almost a quarter of London’s buses—confirmed a cyber-breach had affected software that schedules bus drivers and services.

Additionally, the NHS experienced a major outage following a cyber-attack in August on a third-party vendor. With software offline, doctors had to resort to recording medical notes on pen and paper. It may take several months for the NHS to recover from this attack.

Sadly, the UK isn’t alone in the recent increase in cyber-crime. There’s also been a spate of cyber-attacks across Europe. For instance, Italy’s National Cybersecurity Agency recently warned of increased cyber-threats across the country’s energy operators and infrastructure. This

followed a confirmed cyber-attack on Italian oil company Eni.

### Conclusion

With frequent cyber-attacks affecting multiple organisations, it’s clear no one is immune from the risks of cyber-crime. As such, it’s vital that organisations have cyber-attack response plans in place to ensure quick recovery from potential breaches. Additionally, employers should review their IT systems to ensure adequate security precautions are in place.

For more cyber-security guidance, contact us today.



Contains public sector information published by GOV.UK and licensed under the Open Government Licence v3.0.

The content of this publication is of general interest and is not intended to apply to specific circumstances or jurisdiction. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice from their own legal counsel. Further, the law may have changed since first publication and the reader is cautioned accordingly. © 2022 Zywave, Inc. All rights reserved.