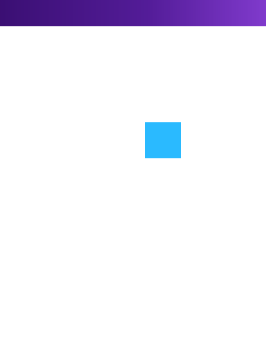


The Escalating Cost of Cyber Insecurity for UK Enterprises

For large UK businesses, cybersecurity is no longer merely an IT concern; it is a critical organisational imperative with staggering financial implications.



This infographic details the true financial burden of cyber attacks on large organisations, highlights the most pressing threats, including the persistent ransomware threat, and offers actionable strategies for building resilience.



High profile 2025 breaches

£3.78 million: the average cost of a data breach for UK organisations in 2025, a figure that dwarfs the general business average and underscores the severe financial risk.

The Jaguar Land Rover cyberattack in late 2025 stands as the UK's most financially devastating cyber event, with an estimated economic impact of **£1.9 billion**.

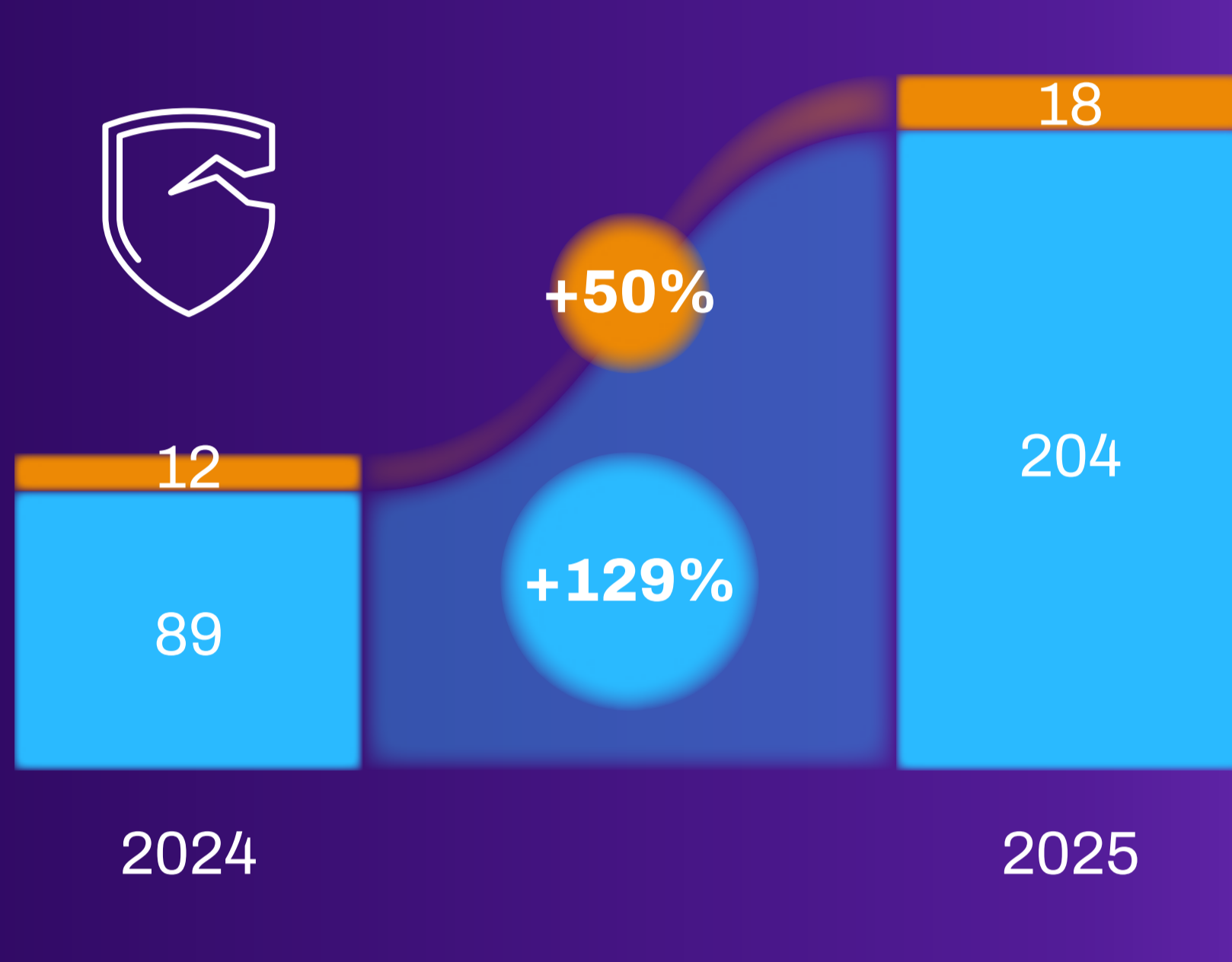
An estimated **£300 million** cost to Marks & Spencer and **£120 million** to Co-op in 2025, further illustrate the catastrophic potential for **operational disruption and reputational damage**.

Attacks of national importance surged in 2025

204 “nationally significant” cyber attacks were tackled by GCHQ’s National Cyber Security Centre in the year to September 2025 – a sharp increase from the 89 that occurred in the previous year.

NCSC incident statistics: Percentage growth (year to september)

- Highly significant incidents
- Nationally significant incidents



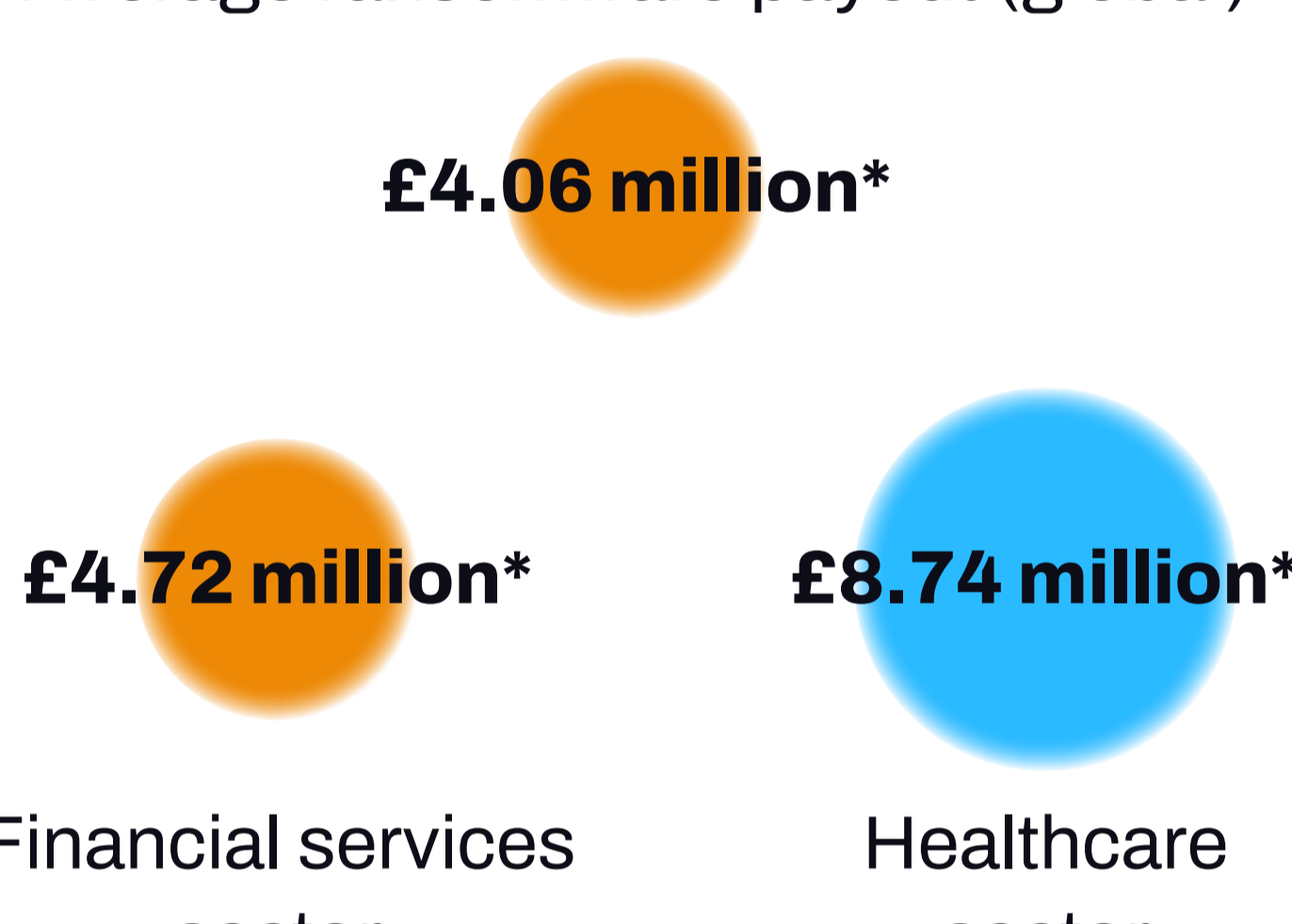
Ransomware: A rising threat

£5.6 million: average ransomware payout among UK businesses, with 1 in 8 companies (12%) paying between £3.95 million and £7.9 million.

These attacks can be particularly devastating for large organisations, particularly in the financial and health sectors, leading to significant operational disruption and financial losses.

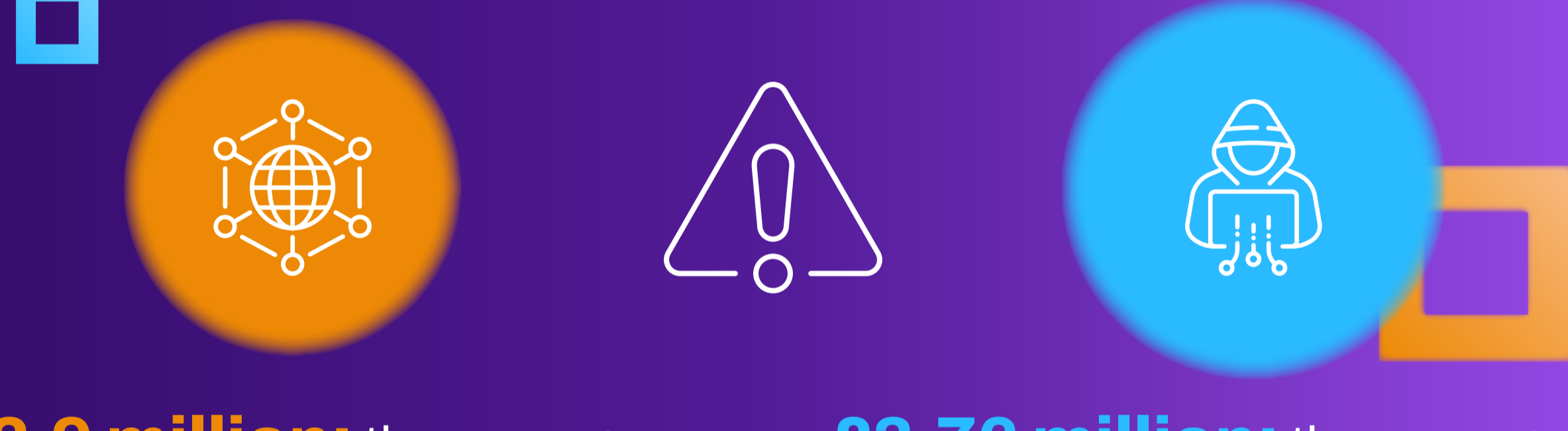
Average cost of ransomware incident (2025)

Average ransomware payout (global)



Breach costs bite – even before severe scenarios

The “data breach lifecycle” – the time it takes to identify and contain a breach – reveals a clear correlation between its length and associated costs.



£2.9 million: the average cost for data breaches globally, with a lifecycle under 200 days, a nearly 5% decline from last year’s £3.05 million.*

£3.76 million: the average cost for data breaches with a lifecycle exceeding 200 days, compared to breaches with lifecycles under 200 days, representing nearly an 8% decrease from last year.

Looking forward – actions that reduce impact

The NCSC urges organisations to become a harder target, emphasising board accountability and robust supply-chain controls as critical priorities.

Globally, AI-assisted security significantly cuts breach costs; for example, breaches with AI security averaged **~£2.6 million**, compared to **~£4 million** without it.

The increasing sophistication of cyber warfare, including the use of advanced persistent threats and zero-day exploits, highlights the **urgent need for proactive defense strategies**.

For UK leaders, focusing on incident readiness, third-party governance, and core security measures like multi-factor authentication are key to mitigating future risks.

Average cost of a data breach (global benchmark)



Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization’s cyber risk exposure in real time.

Sources: Armis, BBC, Bright Defense, CNBC, Cyber Monitoring Centre, DSIT: Department for Science, Innovation and Technology, The Guardian, IBM, Infosecurity Europe, National Cyber Security Centre, UK Home Office

* Note, the figures above have been converted from USD.

<https://www.armis.com/cyberwarfare/>

