Cyber, ransomware and what it means for UK business

November 2025

H/ADVISORS

Introduction

Heathrow Airport, M&S, Jaguar Land Rover, Harrods, and Southern Water are just some of the names that have been targeted by a spate of cyberattacks on high-profile British businesses this year.

A growing wave of cyber incidents has seen the networks of various organisations infected with ransomware causing severe disruption by encrypting or scrambling their data. The M&S cyber incident saw data stolen from thousands of customers and employees, allowing the attackers to compound the retailer's embarrassment by sending the ransom demand directly to its chief executive with an employee's email account. Meanwhile, a late summer cyberattack on Jaguar Land Rover is estimated to have cost the UK economy almost £2bn.

A rising number of organisations are facing a nightmare scenario – rebuild all computer systems from scratch or pay anonymous hackers millions of pounds in ransom for the antidote. Some of the organisations above have refused to say if they paid up or not.

In response, the UK Government is drafting legislation that would make Britain's laws on ransomware some of the strictest in the world. The measures under consideration are:

1. **Mandatory reporting:** requiring organisations to inform UK authorities when they sustain a cyberattack.
2. **Authorisation regime:** mandating private sector organisations to seek permission from UK authorities before making payments to cybercriminals.
3. **Ban on payments:** organisations that are deemed to be part of critical infrastructure will face a complete ban on paying cybercriminals, as will the entire public sector.

If adopted, these measures would match only Australia in their aggressive crackdown on the business model of hackers.

How does the UK's approach compare?

The UK is positioning itself as a leader in tackling ransomware – but there are risks in going too far ahead of international partners. The Government wants to see action at the OECD level or through an international ransomware taskforce, but until there is global momentum it is likely to press ahead alone.

There are challenges in doing so. UK businesses operating internationally will need clarity on whether the legislation applies extraterritorially. The risk of one or two high-profile companies losing jobs because they are unable to secure licences could become poster children for a poorly operating regime.

International cooperation will be vital. The UK has already hinted at alignment with the EU's NIS2 directive, while Australia is expected to move in parallel. The United States and China add a further layer of complexity, with global dynamics shaping how effective UK action will be.

What are the implications for business?

The ransomware measures are fundamentally interventionist. If enacted, they would go much further than any other jurisdiction has attempted in disrupting the ransomware business model.

This is a clear shift in thinking by policymakers. Cyber security is being taken more seriously, with the Bill signalling a willingness to intervene directly. However, this sits awkwardly within the UK's broader cyber security strategy, which tended to take a laissez-faire approach before Russia's invasion of Ukraine and the surge in artificial intelligence sharpened political focus.

If there is to be a stronger push to mandate higher cyber security standards, some are calling for greater business support to balance this, through public-private resilience funding and proportionality measures for SMEs.

There are also concerns that a growing divide will emerge between organisations that can keep pace with AI-enabled threats, and those that fall behind – exposing them to greater risk and intensifying the overall threat to the UK's digital infrastructure.

What happens next?

Ministers and officials are now working to clarify the scope of the proposals, including key questions around enforcement, thresholds and liability.

More detailed guidance will follow before implementation, but organisations – particularly those in the public sector and operators of critical national infrastructure – should start preparing now. With ransomware threats increasing, operational resilience has become a business imperative rather than an option. Organisations need to evaluate their readiness and ensure the right systems, processes, and support are in place to meet forthcoming regulatory requirements.

While there is currently no firm timeframe in relation to these proposals, it appears that the Government is already liaising with regulators and impacted parties to further develop the plans to see how they will fit within the upcoming **Cyber Security and Resilience Bill.**

Businesses will need to review their current compliance efforts and identify gaps against the Bill's requirements. The Bill is expected the scope of the regime to cover more sectors, including digital services and supply chains in previously unregulated sectors. Regulators will gain enhanced powers, including cost recovery mechanisms, proactive investigation capabilities, greater scrutiny of suppliers, new auditing requirements, and even on-site inspections. Looking ahead, the Bill could also expand to cover artificial intelligence, more extensive risk assessments, or exemptions for the military and police.

Royal Assent is expected ahead of the end of the parliamentary session in the spring. Once passed, implementation of the new regime will be crucial. The key question is whether it provides a genuine opportunity to improve cyber security or becomes a compliance burden for businesses.

Best practice communications through a cyber incident

While the regulatory and reporting landscape is changing, the principles of communication during a cyber incident remain the same.

For most organisations, it's a matter of *when* a cyber incident will occur, not *if*. How you communicate with your stakeholders can either strengthen their trust with your organisation.

While all communications advice needs to be tailored to the exact situation, there are five guiding communications principles when responding to a cyber incident:

1. **Communicate early:** It is crucial to communicate at the earliest possible opportunity, once the key facts have been established. This allows your organisation to remain the source of truth, while also controlling the narrative rather than responding to someone else breaking the news.
2. **Be honest, don't speculate:** Be transparent about what you know, but do not speculate. It is better to say you don't have all the information and that investigations are ongoing, rather than potentially correct yourself later.
3. **Be mindful of tone:** It must be authentic and compassionate, but not overly emotional. Remember, your organisation is not the 'victim', the individuals who had their personal information compromised are the victims.
4. **Risk and crisis management is multifaceted:** Don't just focus on one stakeholder group, or divert all your attention to the one which is overly loud. Conduct an audit of your entire stakeholder environment to ensure no one is missed in your communications plan. Managing your stakeholders consistently and simultaneously is key to keeping them on side.
5. **Prepare now:** Organisations can prepare for their response to a cyber incident by scenario planning, undertaking crisis simulation workshops, and drafting materials ahead of time. This will ensure you're not on the back foot when an incident occurs.

Contact

To learn more about how these changes could impact your organisation, or for support in cyber security preparedness, contact the H/Advisors team.

Thank you

Vikki Kosmalska

Partner, H/Advisors Maitland

vikki.kosmalska@h-advisors.global

Mairi Maclennan

Partner, H/Advisors Cicero

mairi.maclennan@h-advisors.global

Roddy Thompson

Consultant, H/Advisors Cicero

roddy.thompson@h-advisors.global

H/ADVISORS