Insight

masonadvisory

Are we taking cybersecurity seriously enough?

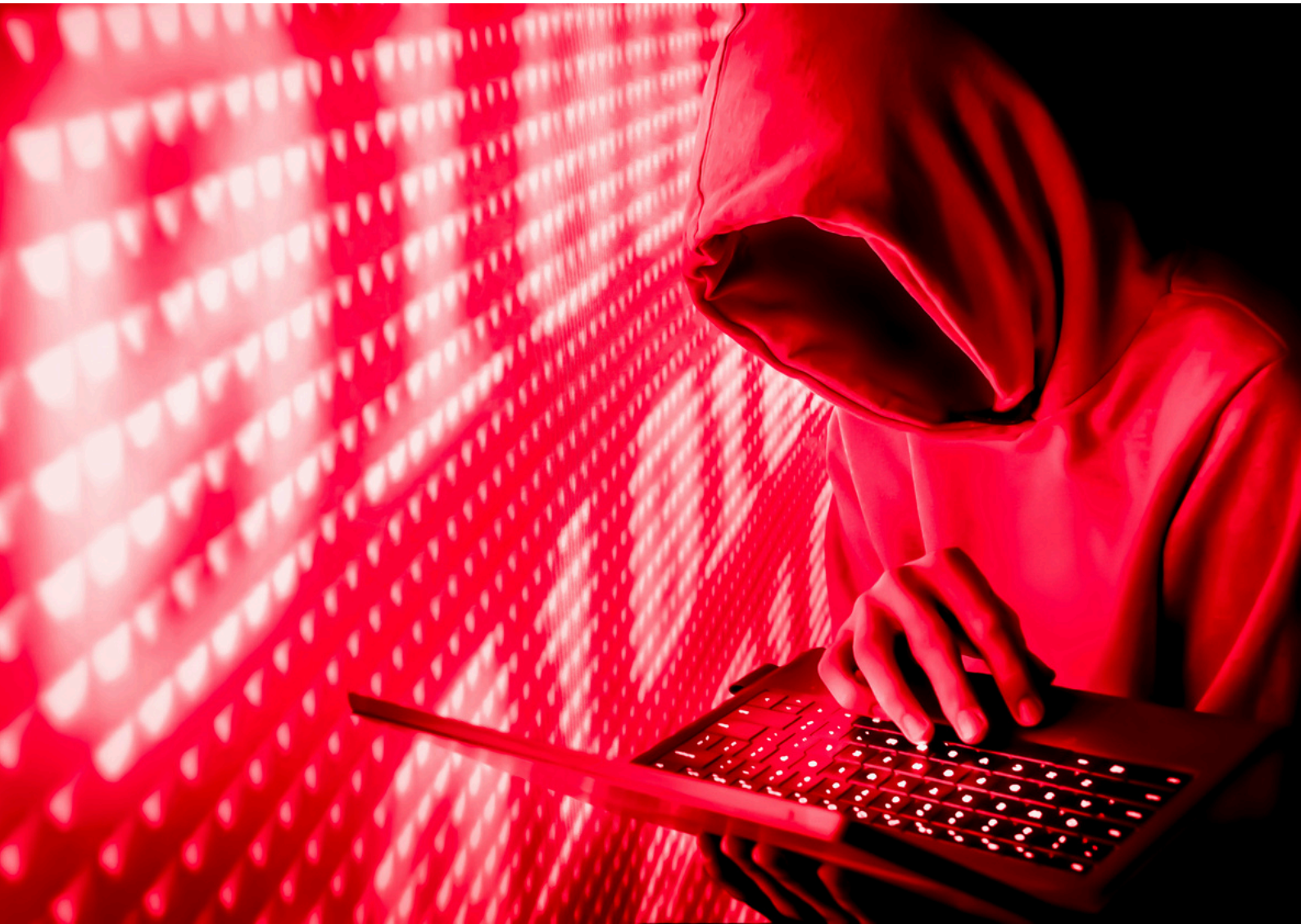
What should organisations be considering to keep their customers and employees safe online and ensure their cyber defences are robust?

Industry

All industries

Services

Cyber



Throughout history, the safety of our people, our families, our communities has been a core value of society. We have always actively built protections into our societies e.g. policing, legal systems and we see it as a responsibility of us all.

Today, that same principle must guide how we protect ourselves in the digital world. Cybersecurity is no longer just the responsibility of the IT department; it is now a business-critical responsibility that underpins customer trust, loyalty and growth.

So why is it that keeping organisations (and their customers) safe online is still often treated as a Technology problem rather than a strategic imperative? Let's investigate what organisations should be considering?

The threat landscape continues to grow and become more sophisticated by the day. There are plenty of new examples in the media on a regular basis, let alone those that we don't hear about. Ransomware is one of the most persistent and publicised threats, data theft continues to rise and exploiting weaknesses in third-party suppliers to gain access to companies' assets is also becoming a wider-utilised tactic. Despite all of this, many organisations remain underprepared, often because of focusing on other priorities such as digital transformation, cost savings and dealing with legacy technology/tech debt.

A key consideration is investment. Across all UK industries, the spend on cyber security ranges between 9–10% of the IT budget (Vanta's State of Trust 2023 report). According to an EY study, the banking industry globally is expecting to allocate 11% of IT budgets to cybersecurity. However, this investment is often spent reacting to external measures such as new regulation/compliance requirements and/or responding to a security incident rather than proactive planning. We often see organisations underinvesting in areas such as security by design, 3rd party risk management and incident response planning.

The investment aspect is quite often a symptom of a larger issue as alluded to earlier; too often cybersecurity is seen as an IT concern and not a wider business objective. Whilst larger and regulated firms generally have a CISO and their security department reporting outside of IT, it is estimated that up to 70% of UK organisations still manage cybersecurity as part of the IT department. (Brian Haugli, CEO SideChannel, 2024).

Cybersecurity resilience is not just about tooling, critically it is about culture, leadership and being prepared. As human beings we generally don't like to spend time, effort and money on something that may not happen. However, we need to accept that cyber-attacks happen on a far more regular basis than we would like to admit, and so we need to be prepared. Organisations need to consider how best to:

- Align security priorities and required spend with business priorities · Ensure that risk is managed pragmatically as well as efficient and effective use of spend.
- Ensure they have a clear understanding of their vulnerabilities and how to remediate them
- Educate their people across the business to be security-savvy.
- Manage their 3rd party partners and vendors to ensure they have robust controls in place.
- Plan out attack scenarios that may need to be considered · Implement and maintain effective enterprise-wide monitoring.

- Ensure ongoing activity is in place to test the organisation's defences, and ensure the effectiveness of communication and crisis coordination

I've managed to get this far without mentioning AI, which only goes to demonstrate the complexity of what we are all having to deal with. As AI adoption accelerates, the threat landscape and the sophistication of attacks is only going to increase.

Unfortunately, there isn't a single silver bullet to dealing with this, but the direction is clear – security needs to be embedded earlier in the thinking, both at an organisation level and in the development cycle. Much like maintaining a digital business, cybersecurity is now part of the everyday business requirements and as a result requires increased ongoing investment.

So, are we taking cybersecurity seriously enough? The evidence and threats suggest not yet but we are on an upward curve. With invested leadership, the right strategy and approach and continuous improvement, organisations can build and maintain the required level of defences to keep themselves and their customers safe. At Mason Advisory our approach to supporting organisations through our Cybersecurity Strategy and Oversight services can help deal with today's challenges and build the resilience to face into tomorrow's.

Author

Mike Kingston
Managing Consultant
email: contact@masonadvisory.com

About Mason Advisory

Mason Advisory has offices in Manchester and London and employs over 100 staff, with plans to continue its expansion. We enable organisations to deliver value through digital & technology transformation, solving complex business challenges, and helping clients set strategy through the intelligent use of IT resources including architecture, cyber, operating model and organisational design, service management, and sourcing. We operate in sectors such as financial services and insurance, legal and law, government, health and social care, emergency services, retail, FMCG, transport, and not-for-profit.

Contact us

To get in touch, please email contact@masonadvisory.com or call +44 333 301 0093

MANCHESTER
Landmark
St Peter's Square
1 Oxford Street
Manchester
M1 4PB

LONDON
Bush House
North West Wing
Aldwych
London
WC2B 4PJ