Insight

masonadvisory

When the human factor fails: rethinking cybersecurity from the inside out

Despite massive investment, organisations remain vulnerable—because no software patch can fix human nature.

Industry

Agnostic

Services

Cyber

The recent well published cyber attacks have led me to reflect on why after all the investment in cybersecurity organisations are still exposed to these attacks.

Some quick research demonstrated that while there remains debate over the exact numbers, most experts agree that over 2 thirds of successful attacks involve a human element, including social engineering, mistakes, or misuse.

Cybercriminals target users because they are often the easiest entry point into a system. Unlike software, which requires technical expertise to exploit, users can be manipulated through psychological tactics. Phishing emails, for example, are designed to appear legitimate, preying on trust and urgency to prompt action. A single click on a malicious link can compromise an entire network.

Moreover, the rise of remote work has expanded the attack surface. Employees working from home may use unsecured networks, share devices with family members, or fail to update their software, creating additional vulnerabilities.

Cybercriminals are quick to exploit these weaknesses, knowing that even the most advanced security systems cannot compensate for human error.

A further factor is training fatigue. Many organisations hold periodic cybersecurity awareness sessions, yet these often fail to leave a lasting impression. When users are bombarded with security warnings, complex password rules, and mandatory training videos, the result can be complacency or even resistance. Cybersecurity is seen as a chore—something for the IT team to worry about—not a shared responsibility.

Despite the billions spent worldwide on cybersecurity the vulnerability to user error remains and the answer lies in human nature. Unlike software, people aren’t programmed to operate within set parameters. We improvise, we get distracted, we forget. This unpredictability makes employees susceptible to social engineering attacks, like phishing emails or phone scams that impersonate trusted figures to extract sensitive information. One misplaced click on a convincing fake login page can compromise entire networks.

Technology alone can’t eliminate this human element. What’s needed is a culture shift. Cybersecurity needs to be woven into the fabric of how people work and think. This means making security principles intuitive, rewarding good behaviour, and ensuring users feel empowered rather than punished when dealing with security-related concerns. After all, when people are afraid of admitting mistakes, breaches go unreported, and threats linger undetected.

Ultimately, an organisation’s security posture is only as strong as its least-informed user. While cutting-edge tools are vital, they must be paired with continuous education, user-centric policies, and an environment where security is everyone's job. Because no matter how advanced our technology becomes, it’s still the everyday choices of individuals that determine whether a breach happens—or doesn’t.

While technology plays a crucial role in defending against cyber threats, users remain the key vulnerability.

Recent ransomware attacks underscore the importance of addressing human error and behaviour in cybersecurity strategies.

By prioritising education, awareness, and proactive measures, organisations can empower their users to become the first line of defence rather than the weakest link.

If you would like to speak to one of our cybersecurity experts regarding the insight article, email contact@masonadvisory.com contact us to discuss further.

If you want to find out more about our services, click here.

Author

David Murton
Principal 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