Cyber risks explained for businesses

Cyber risk is often treated as a technical issue, but responsibility for outcomes sits with the business, not just IT teams or suppliers. This applies to organisations of all sizes. Regardless of who manages systems day to day, accountability remains with the organisation.

Cyber risk goes beyond cyber attacks. It includes loss of access to systems, exposure of sensitive data, operational disruption, and reliance on third parties. Serious impact does not require a sophisticated breach.

Outsourcing IT or security does not remove responsibility. In the event of an incident, customers, insurers, and regulators will expect organisations to demonstrate oversight, awareness of risk, and informed decision making, even where services are delivered by third parties.

Managing cyber risk at a business level does not require technical expertise. It requires clarity around ownership, supplier oversight, and how incidents would be handled in practice.

If you would like to discuss your organisation's exposure or prepare for a cybersecurity assessment, contact **info@sccyber.co.uk** or visit **www.sccyber.co.uk**.

www.sccyber.co.uk
info@sccyber.co.uk