LRQA
Your Risk Management Advantage

CYBER RISK IN PRACTICE
10 ESSENTIALS FOR ORGANISATIONS

DID YOU KNOW THAT LRQA HAS A DEDICATED CYBER FUNCTION?

We work with clients across all industry sectors to deliver industry-leading testing, consulting and assurance services. Our aim is to ensure customers have a clear understanding of their cyber security risks, enabling them to take reasonable and proportionate action to manage those risks in line with their organisational strategic objectives.

Below is our recommended list of the top ten cyber security basics that should be considered as a baseline for all organisations:

1.

Understand the scope of your environment by maintaining an asset register and information asset register.

The asset register covers hardware, software and physical premises. The information asset register details the types of data held, including intellectual property, personal and sensitive data, how it is stored, and who has access.

2.

Promote physical security as best practice, not a hindrance.

View physical premises as layered protection. Ensure sufficient controls are in place at each layer to allow and restrict access appropriately. Consider remote and hybrid workers, including the security of individuals and assets while travelling.

3.

Maintain accurate network and data flow diagrams of your environment.

Alongside the asset registers detailed above, these help identify critical assets, single points of failure, and where potential risks or weaknesses exist.

4.

Back up, segregate and secure data.

Create copies of business-critical data and separate backups from the primary data source, either physically or logically. Maintain access controls to protect backups in line with the original data sources. If systems are compromised by an attacker, backups can be used to restore operational systems.

5.

Leverage technology to enhance your security posture.

Use multi-factor authentication, enable automatic updates and security patching, implement email filtering technologies, and deploy active anti-virus across endpoints and servers. These measures significantly reduce the risk of compromise through common attack methods.

6.

Have an identity and access management (IAM) strategy that meets the needs of internal staff and third-party service providers, without unnecessarily compromising your security posture.

Implement role-based access control (RBAC) so staff only access the resources and data required for their role. Regularly review RBAC controls as part of joiners, movers and leavers processes. Where third-party access is required, restrict it to a point-in-time basis rather than open-ended, unrestricted access.

7.

Conduct technical testing of your environment.

Most organisations conduct at least one penetration test annually, unless required more frequently by their network and perimeter controls, such as a firewall. If the environment is segmented to avoid a flat network, test regularly to ensure those controls remain effective.

8.

Document, maintain and test an incident response plan that covers cyber and operational resilience scenarios.

Assume compromise. Attack tactics, techniques and procedures are constantly evolving. Conduct regular tabletop exercises to simulate scenarios and periodically run realistic incident simulations with trained experts.

9.

Provide general training and awareness for staff, alongside dedicated training for those with security responsibilities.

This can range from basic awareness of phishing and common attack methods for all staff, to dedicated training for helpdesk teams to avoid suspicious calls that could result in an attacker gaining access to internal systems. Project management teams may also require training to ensure security stakeholders are involved from the start of a project, rather than being brought in at the end before go-live.

10.

Align to at least one security standard and determine what gaps and risks exist.

Without a standard to benchmark against, it is difficult to understand risk and opportunity. Physical, technical and procedural controls overlap across common industry standards, which continue to evolve in response to advances in technology and emerging threats.

TALK TO LRQA ABOUT STRENGTHENING YOUR CYBER RESILIENCE →