6 Ways to Improve
Your Organisation's Cyber Resilience

Phriendly Phishing

1 STRESS TEST YOUR INCIDENT RESPONSE PLANS

Collate & review your:

- Cyber Security Incident Response Plan
- Incident Response Playbooks
- Supporting crisis management documents.

2 EMBED INTERNAL & EXTERNAL THREAT MONITORING

- *Internal monitoring* should include logs from critical systems & applications.
- *External monitoring* should include dark web monitoring for references to the organisation on underground channels & regular collection.

3 CONDUCT A PERSONAL INFORMATION AUDIT

Review what personal information your organisation is:

- Storing
- Where it is saved
- How long it is retained
- How it is accessed, & by whom

4 UNDERSTAND YOUR EXPOSURE TO THE INTERNET

Manage your attack surface by understanding which of your organisation's applications & systems are exposed to the internet.

5 REVIEW YOUR CYBER SECURITY RISK PROFILE

Work across your executive & technical leaders to:

- Identify your cyber risks & address each specifically
- Ensure that they have been mitigated – where this is not possible residual risk positions must be accepted by the organisation

6 ELEVATE YOUR CYBER HYGIENE TRAINING & EDUCATION

Training & testing staff to ensure that cyber security remains an organisation-wide priority is critical to:

- Ensure that gaps in your cyber defence are avoided
- Increase the likelihood that attacks are detected & disrupted

As the cyber threat environment continues to evolve, these six steps will help build a stronger, more secure foundation to your cyber security strategy.

Read the full CyberCX blog here.