

CYBER CRISIS SELF-ASSESSMENT CHECKLIST

The following checklist is designed to help you identify specific vulnerabilities and gaps in your organisation as it relates to cybersecurity crisis management. Through this assessment, you will gain valuable insights into areas that require attention and improvement to enhance your preparedness for potential cyber crises.

PREVENT

- Has an 'issues register' been created which captures scenarios and implications that may arise from a cyber breach?
- Has the business comprehensively assessed its readiness to face these potential scenarios?
- Has the business prepared to provide plans, processes and effective communication to all team members in the event of a cyber breach?

PREPARE

- Does the business have a tailored incident response plan for cyber breaches?
- Is there personnel and technology available for prompt breach detection and response?
- Are designated cyber crisis management employees trained to respond effectively?
- Are the CEO and/or Board members trained to handle cyber crises?
- Is there a preparedness to transparently communicate with stakeholders post-breach?
- Are notification protocols prepared for individuals, regulators, and law enforcement?
- Are external cybersecurity experts engaged for incident response?
- Is there cybersecurity insurance covering communication and reputation damage?

PRACTICE

- Has the business conducted public relations exercises or simulated crisis scenarios for cybersecurity breaches?
- Are there strategies to analyse and learn from previous incidents to refine response plans and actions?
- Is there ongoing training for designated cyber crisis management teams to re-skill and respond to specific crisis situations?

To enhance your organisation's readiness for a cyber crisis, focus on implementing identified improvements, conducting training and drills, and collaborating with external cybersecurity experts for incident response support. Click [here](#) to learn more about how BlueChip can help your organisation prepare for a cyber crisis.