Business Continuity Management for Cyber Risk

Supporting digital technology from the challenges of disruptive cyber events.

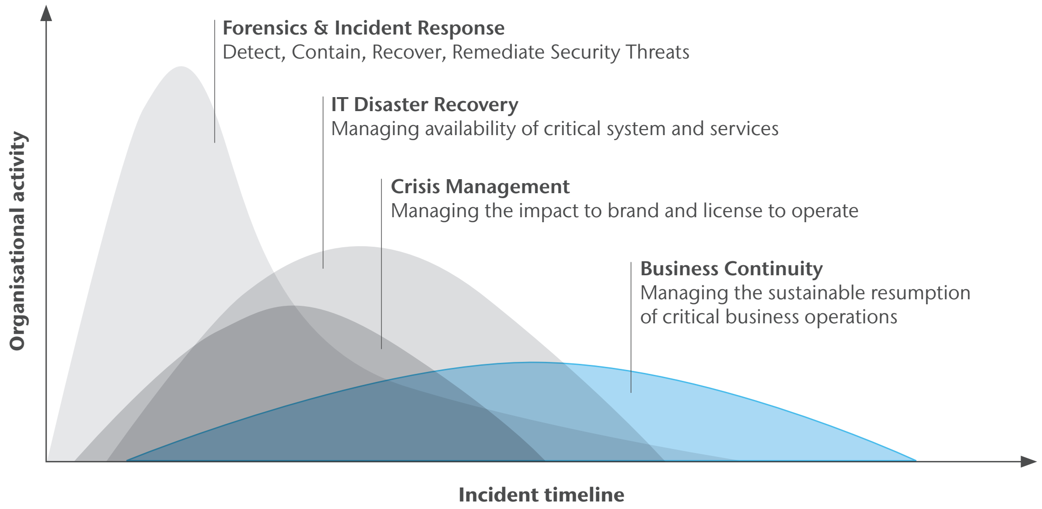
Accelerated digital transformation and the adoption of 'Industrial Internet of Things' (IIoT) has exposed organisations to a variety of disruptive cyber attacks. As this transformation continues, it's now vital that exposures to ransomware and disruptive cyber events are addressed as a priority within business continuity planning.

But not all organisations have upgraded their legacy Business Continuity Management processes to counteract cyber attacks to mission-critical systems – and the potential operational and reputational losses that could result.

The technology and threat landscapes continue to evolve. Threat Actors are upping their game and exploiting critical dependencies on digital technologies. This is highlighted by ransomware claims increasing by 340% since 2018.[1]

At the same time, Cyber Insurers are seeing an increase in losses from disruptive cyber events in an already hardening market. This is resulting in reduced capacity, rate increases, and greater scrutiny on an organisation's BCM plans. We help organisations be more 'market-ready' by reviewing their risk reduction processes to enable them to demonstrate an ability to respond to disruptive events.

Business continuity determined by activity and timeline



How Aon can help

Aon's Business Continuity Management for Cyber Risk solutions helps identify gaps in legacy BCM strategies that have emerged due to the rapid adoption of digital technology.

An updated and upgraded Business Continuity Plan that addresses the commercial dependency on digital technology mitigates future operational disruptions and financial losses from disruptive cyber attacks.

We also support companies to better align their existing Business Continuity Plans to real-life cyber scenarios to determine an organisation's current level of resiliency and improvement requirements.

To learn how Aon can empower results for your organisation contact:

Adam Peckman
Global Practice Leader
Cyber Solutions
adam.peckman@aon.co.uk

David Molony
Director of Cyber Risk
Consulting EMEA
david.molony@aon.co.uk

Mani Dhesi
Head of Growth and
Innovation
Commercial Risk Solutions
mani.dhesi2@aon.com

aon.co.uk

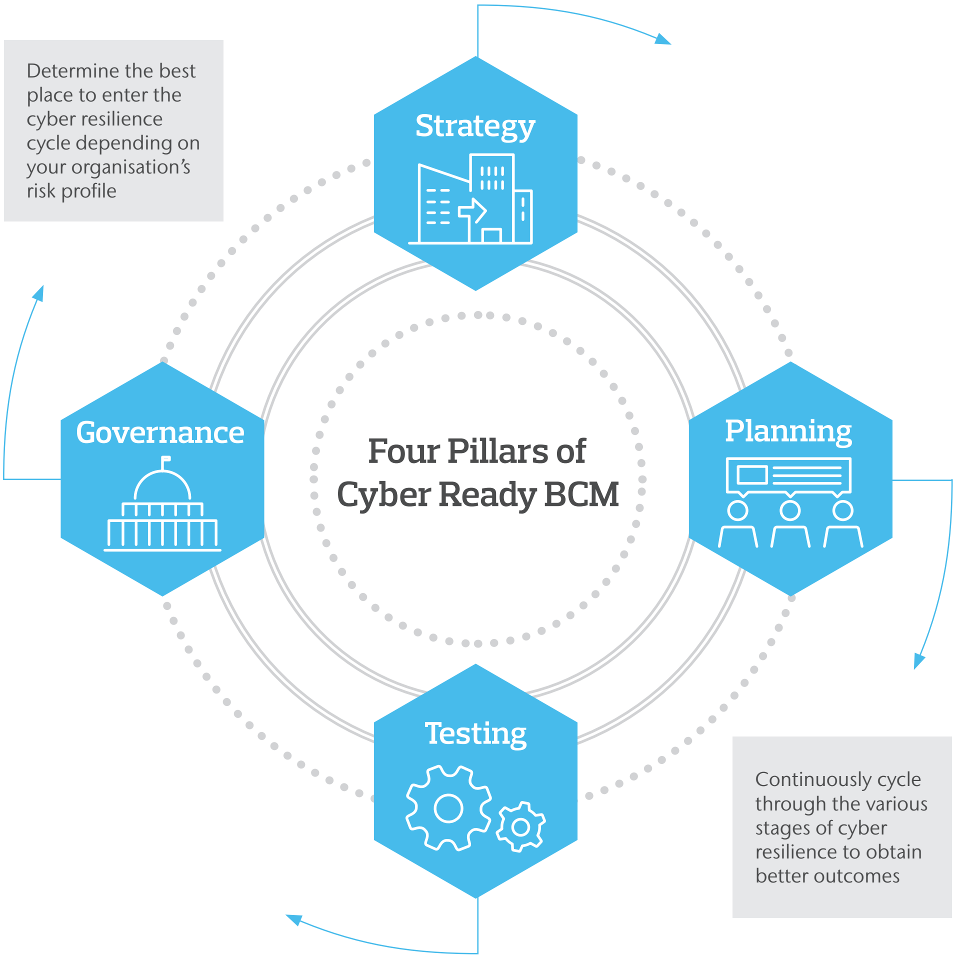
Empower Results®

---

[1] *Calculated on a retrospective annual basis using data supplied to Aon's Claims Analytics team 2020.*

Our approach

- **Diagnostic and Strategy:** A proprietary maturity assessment to determine if existing BCM strategies address current technology dependencies and emerging cyber threats
- **Planning:** A comprehensive evaluation/audit of any existing BCP to address disruptive cyber scenarios impacting critical technology
- **Testing:** A bespoke table top exercise or simulation exercise to test awareness and effectiveness of BCPs in a real-life setting
- **Governance:** The development of new internal governance structures to better support a revised cyber-focused BCM programme



Determine the best place to enter the cyber resilience cycle depending on your organisation's risk profile

Continuously cycle through the various stages of cyber resilience to obtain better outcomes

Key benefits

- Reducing frequency and potential severity of disruptive cyber events
- Determining the critical dependencies of revenue generating operations/teams on digital technology
- Increasing organisational resilience to disruptive cyber events which may reduce unbudgeted losses
- Improving insurer perceptions of the risk profile to unlock broader coverage and competitive terms
- Focusing commercial needs and business continuity requirements with Incident Response plans
- Understanding continuity response priorities for vendors, customers, partners and regulators that are triggered by a cyber event
- Linking investments in cyber resilience with the technology dependencies of the business to justify future CAPEX
- Establishing an appropriate Risk Governance architecture that covers disruptive cyber events

Aon UK Limited is authorised by the Financial Conduct Authority (FCA) for insurance activities. The services described in this document are not regulated by the FCA. FP.AGRC.360.AP

Empower Results®