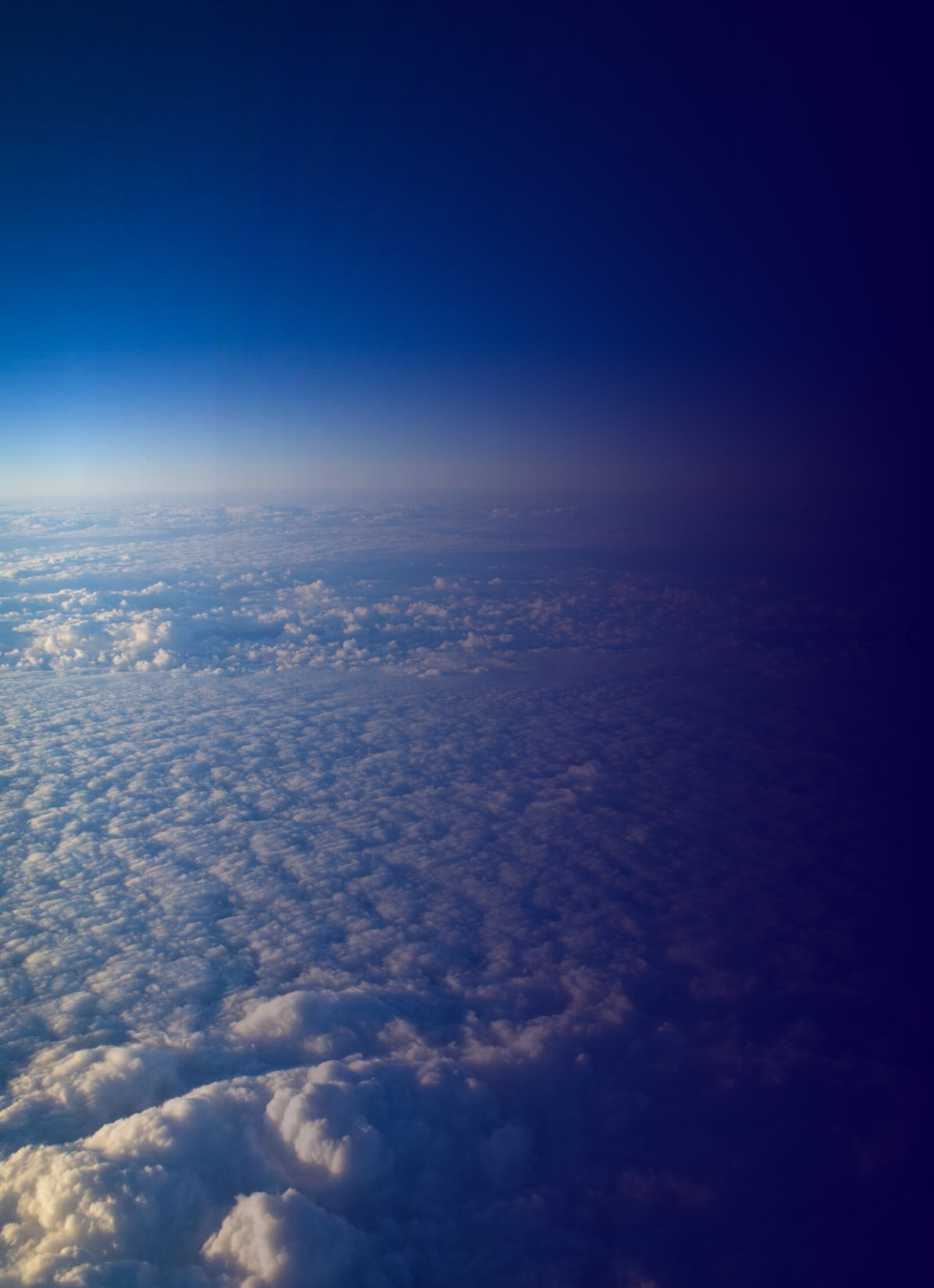

BEYOND blue

# GCLOUD 14 SERVICES

## CYBER RISK

# About Beyond Blue

## Beyond Blue partners with clients to tackle their most complex cyber and resilience challenges.

Beyond Blue was formed by MD David Ferbrache OBE and Chairman Paul Taylor CBE, each having over 30 years experience in cyber security and resilience.

We are an award-winning boutique consultancy who specialise in helping our clients tackle their most difficult cyber and resilience challenges and seek to equip organisations with pragmatic toolkits to prepare for, respond to, and navigate through this landscape.

Our team has broad and diverse experience in cyber security, technical architecture, crisis management, cyber investigations and Operational Resilience, from both private and public sector backgrounds.

We work across a variety of industries including financial services, government and national security in the UK, Ireland, Middle East and Asia.

The team engages at all levels but specialises in assisting and advising boards and senior management, with first-hand experience dealing with the unique challenges cyber and resilience poses for leadership while helping clients embrace the opportunities offered by emerging technology.

## We have a passion for...

**SOLVING COMPLEX CYBER AND RESILIENCE PROBLEMS**

**DEVELOPING CUSTOMISED INNOVATIVE SOLUTIONS**

**HARNESSING DIVERSE TALENTS FROM DIFFERENT SECTORS**

## AWARD WINNING

Cyber Security Awards
Winner 2018

CIR
WINNER
BUSINESS CONTINUITY AWARDS 2022
STRATEGY THROUGH PARTNERSHIP

BCI Europe Awards 2022
WINNER!
bci Leading the way to resilience

## SUPPORTING

ARMED FORCES COVENANT
EMPLOYER RECOGNITION SCHEME
BRONZE AWARD

# Prepare for a complex, digital future

**We recognise that every business functions within its own unique setting. To address this, our strategy meticulously evaluates the risk and threat landscape across government, business and industry. Below is an outline of our three-tiered offering:**

## Operational Resilience

Help clients define Operational Resilience strategies and frameworks, with expertise in scenario testing, data resilience and enterprise response & recovery. Working with clients to design resilient business solutions which can be robust to threats, hazards and incidents; as well as meeting regulatory needs.

## Cyber Strategy

Expert insights in the development of organisational (and national) cyber security strategies and policies, harnessing the opportunities offered by emerging technologies. Robust cyber risk assessment methodologies and approaches informed by a deep understanding of the developing cyber threat.

## Board and Executive Exercising

Guiding clients in crisis methodology and response plans. Bespoke cyber incident exercises providing specific value to clients tailored to their individual needs and challenges. Exercises which consider their threat and operational environment with facilitators experienced in executive engagement.

| | Operational Resilience | Cyber Strategy | Board and Executive Exercising |
|---|---|---|---|
| **Offering** | – Strategy & Target operating model (TOM) definition for operational resilience and business continuity functions<br>– Important business service (IBS) identification and impact tolerance (ITOL) setting<br>– Scenario testing execution, including third party scenario testing and assurance<br>– Data resilience strategies<br>– Remediation and enterprise response & recovery strategies<br>– Regulatory compliance with UK Operational Resilience Policy, the EU Digital Operational Resilience Act and closely related global operational resilience regulations | – Expert consultancy for the formulation of national and organisational cyber security strategies<br>– Development of national policies relating to emerging technologies and changing threat landscapes, including assessment of policy effectiveness and impact<br>– Frameworks for considering trends and drivers which shape the future cybersecurity landscape including the changing threat and risk landscape<br>– Risk assessment methodologies which are tailored to the client's operational and threat environment, including the evolving ransomware threat in the cloud/3rd party space. | – Creation and facilitation of tabletop and simulated cyber crisis exercises covering a wide range of threats for organisations harnessing cutting edge technology.<br>– Post exercise reporting detailing key themes, what worked well and potential areas for improvements, with associated remedial actions.<br>– Board and executive coaching and education sessions.<br>– Education and awareness to support embedding a positive and effective security and resilience culture across the organisation. |
| **Differentiators** | – Extensive experience of government and defence<br>– Award winning scenario testing methodology<br>– Working with clients to manage resilience in the cloud<br>– Unique insights into third party resilience challenges | – National, sector and organisational risk management experience including modelling of threats, attack vectors and risks employing MITRE ATT&CK methodologies.<br>– Comprehensive ransomware readiness framework. | – Track record of delivery and facilitation across multiple sectors, including private and public sector.<br>– Extensive executive/board engagement experience.<br>– Facilitating at national, sector and organisational level. |

# Our credentials – Cyber Strategy

## Cyber Strategy

Expert insights in the development of organisational (and national) cyber security strategies and policies, harnessing the opportunities offered by emerging technologies. Robust cyber risk assessment methodologies and approaches informed by a deep understanding of the developing cyber threat.

**Offering**

- Expert consultancy for the formulation of national and organisational cyber security strategies
- Development of national policies relating to emerging technologies and changing threat landscapes, including assessment of policy effectiveness and impact
- Frameworks for considering trends and drivers which shape the future cybersecurity landscape including the changing threat and risk landscape
- Risk assessment methodologies which are tailored to the client's operational and threat environment, including the evolving ransomware threat in the cloud/3rd party space.

**Differentiators**

- National, sector and organisational risk management experience including modelling of threats, attack vectors and risks employing MITRE ATT&CK methodologies.
- Comprehensive ransomware readiness framework.

**National and Sector Cybersecurity Strategies**

— Developed national cyber security policies and standards frameworks in areas as diverse as smart cities, internet of things and artificial intelligence helping nations harness emerging technologies in safe, secure and robust ways.

**National Cybersecurity Risk Modelling**

— Helped national agencies review and update national cyber security performance management framework and metrics developing national cyber risk management frameworks and helping sectors and organisations tailor their control environments.

**Organisational Risk and Ransomware Readiness**

— Applying comprehensive ransomware readiness risk assessment approaches to help focus investment in control improvements to counter a rapidly changing threat.

BEYOND blue

# Ransomware Readiness Framework

Interconnectedness and dependency on technology continues to increase, offering a much greater surface and opportunity for cyber-attacks. Ransomware is one of the top threats to organisations and as these attacks become more sophisticated, there is an increasing need for organisations to bolster their cyber resilience posture.

Beyond Blue developed this framework as a recommendation for preparing, responding and recovering from a ransomware incident. This list is not exhaustive but provides the basis of a proactive ransomware strategy, which aims to reduce the risk of a ransomware attack destabilising, disrupting and at worse destroying business operations.

| | Prepare & Protect | Detect & Respond | Recover |
|---|---|---|---|
| Operational | — Understand the Threat<br>— Create Policies<br>— Build a Secure Culture<br>— Resilience by Design<br>— Cyber Insurance<br>— Create Plans & Playbooks<br>— Test Plans & Cyber Exercising<br>— Build Relationships<br>— Supply Chain Management<br>— Recovery Order | — Internal Communication<br>— External Communication<br>— Reporting<br>— Ransomware Negotiation Strategy<br>— Disruption to Customers<br>— Crisis Management Structure<br>— Intel Sharing | — Investigations<br>— Lessons Identified<br>— Share Lessons<br>— Return to Business as Usual |
| Technical | — Incorporate Threat Intelligence Feeds<br>— Assess threat Detection Capability<br>— Multi-Layered Defence<br>— Data Classification & Encryption<br>— Asset & Configuration Management<br>— Backup<br>— Environment Hardening<br>— Patch Management<br>— Vulnerability Management | — Defensive Tooling<br>— Monitor & Analyse Logs<br>— Containment & Isolation<br>— Authentication Protection<br>— Incident Response / Blue team<br>— Check for Decryption Keys<br>— Secure & Preserve Evidence | — Forensic Analysis<br>— Remain Vigilant<br>— Utilise Recovery Order<br>— Backup & Restore<br>— Endpoint Rebuild<br>— Lessons Identified |