



# Cyber Security Advisory

## QinetiQ Digital Resilience

Political risks, bribery, oil prices and financial market fluctuations are among chief concerns for businesses across the globe. Whilst many of these are easily understood and can be easily analysed in terms of their impact on an organisation the impact of cyber security often proves comparatively difficult to measure and quantify.

QinetiQ recognises that it is necessary for organisations to understand not just the external and internal threats posed by cyber-attack, but also an organisation's appetite to accept the risks inherent with these threats. It is also important for these threats to be translated and easily digestible at board levels, to enable organisations to take the appropriate actions and to understand their level of maturity and confidence in relation to digital resilience.

QinetiQ's Cyber Security Advisory service looks to work with senior board members and business leaders across an organisation, to share a clear understanding of the threats that a customer faces, articulated in the context of the business impact they carry. With this understanding, advice can then be given as to the best course of action for an organisation to take to reduce the business impact and to increase confidence in the resilience of their digital platforms to cyber-attack.

The service follows four key principles to personalise the service and deliver exceptional security value. They are:

### **Threat Identification**

Drawing on our wider threat intelligence capabilities and pulling together a situational awareness picture from across our digital resilience service, QinetiQ is able to model the threats an organisation faces from its use of digital systems.

QinetiQ recognises that this is a rapidly developing area and that cyber-attacks are becoming more sophisticated and commonplace. As organisations move more of their operations to digital systems, understanding the resulting threats they face is of critical importance.

### **Business Context**

Understanding the threats faced by an organisation as a consequence of their use of digital platforms is important, but being able to translate these into business context and to prioritise them against organisation's risk appetite.

QinetiQ's service works closely with the business to constantly maintain a prioritised set of real world threats, clearly demonstrating to board members the business impact and context of each.

### **Risk Mapping**

By understanding the threats an organisation faces and by translating these into the business context, it is then important to map these through to tangible, quantifiable risks.

It is at this stage that QinetiQ works with an organisation to understand the level of acceptable risk a business will accept and what this means in terms of the threats they face from cyber-attacks. A clear mapping is shown between business assets, whether digital systems, critically important data or operational processes, and the threats that each faces in a dynamic manner.

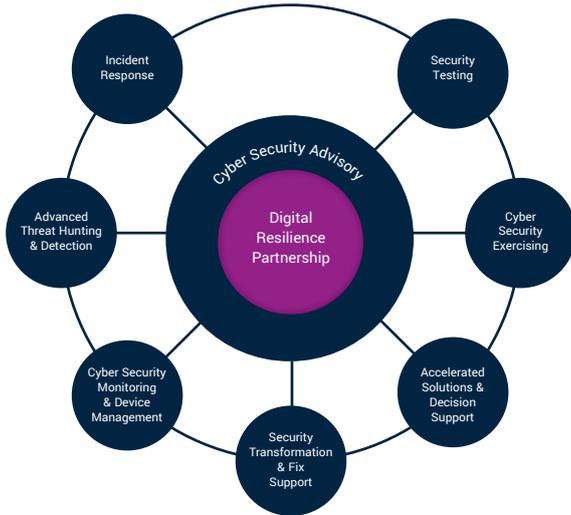
### **Strategic Guidance**

This allows the QinetiQ service to advise board members on the types of mitigations they need to adopt and the strategic direction they need to take. This advice can be used to direct investment and operational spend to maximise resilience and increase confidence across the organisation.

## Digital Resilience

This service forms part of a wider service portfolio, which seeks to help organisations mature their digital resilience and to help build confidence in their ability to deal with cyber-attacks, through a holistic approach. The main integration points for this particular service are:

- **All Services** - This service provides information and direction to the other services in the portfolio, helping to shape further services deliver to address key business concerns



## Key Features & Benefits

---

**Strategic Planning** - Advice to board members on the steps to take and the areas to invest in to improve their organisation's overall resilience to digital compromise

---

**Resilience Confidence** - Helping organisations build confidence in their resilience to digital compromise, able to translate technical threats and risks into business context for senior members

---

**Understanding of the Threat** - Clear understanding of the digital threats an organisation faces and assessment of the impact each would cause on the organisation's operations

---

**Intelligence-led** QinetiQ's extensive exposure to a variety of targeted industries provides us with an excellent insight across the cyber threat landscape.

---

## Collaborating with QinetiQ

At QinetiQ we bring organisations and people together to provide innovative solutions to real world problems, creating customer advantage.

Working with our partners and customers, we collaborate widely, working in partnership, listening hard and thinking through what customers need. Building trusted partnerships, we are helping customers anticipate and shape future requirements, adding value and future advantage.

[www.QinetiQ.com](http://www.QinetiQ.com)

Copyright QinetiQ Ltd 2019 | CYBER SECURITY ADVISORY

### For further information please contact:

Cody Technology Park  
Ively Road, Farnborough  
Hampshire, GU14 0LX  
United Kingdom

+44 (0)1252 392000  
customercontact@QinetiQ.com  
www.QinetiQ.com

QinetiQ/19/01809