ATTICUS communications

UK Government Cyber Security Strategy: 2022-2030 Summary

Atticus Communications: Government Cyber Security Strategy Summary

Overview

The Integrated Review (March 2021) and the National Cyber Strategy (December 2021) set out the government's ambition to firmly establish the UK as a democratic and responsible cyber power, able to protect and promote its interests as a sovereign nation in a world fundamentally shaped by technology. The UK's legitimacy and authority as a cyber power is however dependent upon its domestic cyber resilience, the cornerstone of which is government and the public sector organisations that deliver the functions and services which maintain and promote the UK's economy and society. Whilst the Government has made progress, gaps remain in the Government's cyber resilience, as highlighted by the volume of cyber-attacks towards the Government and the public sector. Backed by £37.8 million of investment, the Cyber Security Strategy explains how the government will ensure that all public sector organisations will be resilient to cyber threats.

Vision, aim and affected public sector organisations

The strategy's vision is to ensure that core government functions - from the delivery of public services to the operation of National Security apparatus - are resilient to cyber-attacks, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.The strategy considers all public sector organisations which are responsible for delivering the Government's core functions, including government departments, arms length bodies, agencies, and local authorities.

To achieve its vision the strategy pursues a central aim - for government's critical functions to be significantly hardened to cyber-attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.

Strategic Pillars

The Government's approach to achieving a cyber resilient public sector is centred around two strategic pillars; building a strong foundation of organisational cyber security resilience and to 'defend as one'.

Building a Strong Foundation of Organisational Cyber Security Resilience

The first pillar aims to ensure that government organisations have the right structures, mechanisms, tools, and support in place to manage their cyber security risks. This will be underpinned by the adoption of the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) as the assurance framework for government, with government specific CAF profiles that articulate the outcomes required by government organisations to proportionately respond to the varying threats to their most important functions. It will be for lead government departments to adapt and apply such an approach in a way that is most appropriate for the public sector organisations within their scope.

Defend as One

The second pillar recognises that the scale and pace of the threat demands a more comprehensive and joined up response, government will harness the value of sharing cyber security data, expertise, and capabilities across its organisations to present a defensive force disproportionately more powerful than the sum of its parts. It will be underpinned by the establishment of a Government Cyber Coordination Centre (GCCC). As a joint venture between the Government Security Group, the Central Digital and Data Office and the NCSC, the GCCC will work to better coordinate operational cyber security efforts, transforming how cyber security data and threat intelligence is shared, consumed, and actioned across government.

Objectives

The pillars are supported by five objectives that set the dimensions of cyber resilience, providing a consistent framework and common language that can be applied across the whole of government.

Manage cyber security risk

Identifying, assessing, and understanding cyber security risks will be key in order to effectively manage them. The foundation of this lies in the visibility and understanding of assets, their vulnerabilities, and the threat to them - whether internal to an organisation or emanating from its supply chain. Clear accountability and robust assurance will ensure that risk owners are aware of the risks they have the responsibility to manage, and that they are doing so appropriately. There will be cross-government information sharing to provide a central view of critical vulnerabilities that will enable cross-government risks to be identified and managed, facilitating rapid mitigation at scale.

Protect against cyber attack

To adopt a proactive and protective stance against cyber-attacks, the Government will develop its shared capabilities, tools, and services to address common cyber security issues at scale, improving cyber security across the whole of government as well as driving efficiency and value for money. At the heart of this is data protection, as well as appropriately classifying information

Detect cyber security events

Building on the risk management and protective measures, the Government plans to develop its capability to detect cyber security events across every part of its estate to ensure that risks can be mitigated before they critically impact government functions and services.

This means having the capability to monitor systems, networks, and services to detect cyber security events before they become incidents. Enhanced coordination will enable government to have the agility to use these data inputs to detect at pace and scale, facilitating coherent responses as well as providing the capabilities to detect more sophisticated attacks.

Minimise the impact of cyber security incidents

As a result of the first three objectives, in hopefully rarer instances where cyber-attacks do occur, the Government will be fully prepared and able to respond to cyber incidents with the capability to restore affected systems and assets and resume the operation of its functions and services with minimal disruption. A critical component of this will be establishing the mechanisms to test and exercise incident response plans, both at an organisational level and across Government.

Develop the right cyber security skills, knowledge, and culture

Achieving this strategy's vision and aim will not be possible without cultivating the required cyber security skills and knowledge, as well as fostering a cultural shift in cyber security across the whole of government. Government will have a comprehensive understanding of its cyber security skills requirements and will incentivise and promote government cyber security careers. Fundamentally, the strategy aims to recognise the importance of cultivating a cyber security culture that empowers its people to learn, question and challenge to drive continuous improvement.

ATTICUS
communications

For more information on how Atticus can help your organisation navigate 2022 please get in touch.

info@atticuscomms.com
AtticusCommunicationsLtd
@AtticusComms
atticuscomms.com