APMG International™ CDCAT®

APMG International

The Challenge

About CDCAT®

The Defence Science and Technology Laboratory (Dstl) developed CDCAT® as a way to help organisations assess their readiness to defend against cyber threats and identify the risks which should be addressed. A commercialisation opportunity was recognised during its initial design and assessment phase, with the tool now being licensed to APMG.

The Dstl Cyber Vulnerability Investigation (CVI) team has been conducting cyber analysis on behalf of a number of Lead Government Departments (LGDs) including the Department for Transport (DfT), Department for Energy and Climate Change (DECC) and the Department for the Environment, Food & Rural Affairs (Defra). Each of the LGDs had a subtly different requirement so Dstl needed a consistent set of Industry Best Practice standards to help understand the sectors and CDCAT® was the tool selected.

What were the departments trying to achieve?

The LGDs involved were trying to get a better understanding of sector maturity and the principal blockers e.g. Training, Personnel, and Organisational that might stop them from reaching a higher level of maturity. The ability to compare a number of assessments against one another using common criteria enabled an understanding of both the overall sector maturity and also the range of maturity across the individual companies.

What types of systems were assessed?

The assessments conducted have covered a mixture of corporate IT infrastructure and also Operational Technology (OT) including Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

SOLUTION

How long did the process take?

In general the CDCAT® Assessment took less than 2 hours to conduct whilst on site and then required further analysis and tailoring of the reporting to include in Dstl reports to LGD customers. Typically the CDCAT® assessment was carried out as part of a wider site visit including a tour and more generalised discussions with the company involved in order to develop a greater understanding of their business, their technology use and relevant sector challenges or concerns.

How easy was it to use CDCAT®?

The data collection aspects of the CDCAT® assessment were easy to carry out using the .NET tool but relied on a suitably qualified and experienced consultant in order to conduct the assessment and capture the data effectively. An even greater level of knowledge and experience was required to interpret the results and also to brief them back to specific companies that took part in the assessments. The tool is effective when applied correctly by personnel with relevant training, qualifications and experience.

RESULTS

How did CDCAT® help?

A number of the individual companies' realised direct benefits from the assessments by exploiting the results of the CDCAT® assessments to provide evidence for mitigation activity or an increased emphasis on cyber security within the company.

Department for Transport (DfT)

The Department for Transport (DfT) has worked with Dstl in order to apply the CDCAT® tool to assess and compare security across a range of assets in the transport sector to inform DfT policy. This work has identified the CDCAT® tool to be useful as part of a wider cyber security programme in helping to identify key cyber security issues and provide an assessment of sector maturity.

Department for Transport

Department for Energy and Climate Change (DECC)

The Department for Energy and Climate Change (DECC) focused the Dstl project toward its responsibilities under the Directorate of Nuclear Resilience and Assurance and the associated NDA Estate. Five organisations underwent an assessment in 2016 to establish a baseline of how the 17 most effective control measures for cyber defence had been implemented. The assessment built upon previous industry assessments for ISO27001 with a focus on how they were implemented and their effectiveness. The CDCAT® assessments identified good practice in the sector and provided organisations with recommendations on how they could strengthen their cyber security. The reporting process also provided estimated financial risk information to DECC which was considered valuable by the assessed organisation as they illustrated a tangible risk.

The Civil Nuclear Sector organisations were not aware of CDCAT® initially, but when introduced and run through with them in a cyber security workshop, they understood the benefits of a structured tool such as CDCAT® and how it could help them direct their cyber resource efforts more effectively.

The assessment work informed and influenced DECC's civil nuclear cyber strategy.

Department of Energy & Climate Change

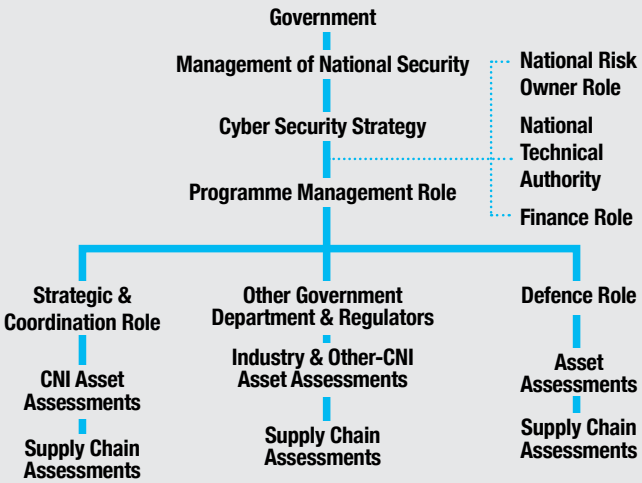
Cabinet Office

Between January 2015 and August 2016, the Cabinet Office used the Cyber Defence Capability Assessment Tool (CDCAT®), to deliver cyber assessments for business-critical assets across the Public Sector, including central Government assets that form part of the UK Critical National Infrastructure.

Using CDCAT®, which was developed by Dstl and delivered by APMG, the Cabinet Office has been able to assess the overall cyber defence capability for a variety of different critical systems within Government. CDCAT® allowed various Departments to gauge how effectively they were implementing their most important security controls, and gave them a starting point for any future remedial work that might need to be considered. The Cabinet Office presented this data quarterly, via aggregate reports that allowed benchmarking across Government, showing themes and trends.

Cabinet Office funded a number of enhancements to CDCAT® that can provide a "Government Grade" high level view of the strengths and weaknesses across Government assets, identifying where changes may need to be made, or if modifications need to be implemented. CDCAT® also enables an overall view of how effectively the budget for cyber defence is being used, which can then inform the efficient and appropriate allocation of funds.

CDCAT® in Critical National Infrastructure (CNI) Cyber Security Risk Assessment - UK Example



 This work was sponsored by the MOD ISS NTA

FOLLOW US ONLINE

@Cyber_APMG

company/apmg-international

APMG International

www.apmg-international.com/cyber