

A photograph of two medical professionals, likely radiologists, looking at multiple computer monitors displaying axial CT scans of a human brain. One person's hand is pointing at a specific scan on the right monitor. The interface includes a menu bar with 'File', 'Edit', 'Project', 'View', 'Window', and 'Help'. The text 'Medical Research Environment v2.0.556' is visible in the top right corner of the software window. A large yellow semi-circular graphic is overlaid on the bottom left of the image.

Building resilience and strengthening cyber procurement

Power to your **procurement**

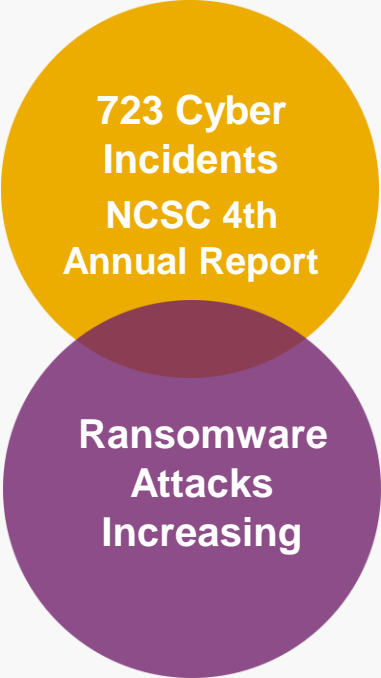
Agenda

- overview
- 5 steps to build resilience and reduce disruption
- procurement's role in cyber security



Overview

- significant increase in cyber attacks since the beginning of the pandemic
- changes in how we work - a move to homeworking, unsecure networks and opportunistic cyber criminals exploiting the situation
- impact is hugely detrimental - data loss, inability to operate, reputational damage, financial loss and emotional toll on employees



723 Cyber
Incidents
NCSC 4th
Annual Report

Ransomware
Attacks
Increasing

5 steps - build resilience and reduce disruption

Power to your **procurement**



Crown
Commercial
Service

Step 1

Understand critical assets

- a good understanding of the assets in your IT estate and strong asset management processes to ensure information is up to date
- understanding of the data held in systems, the “value” of that data to an outside party and impact if it got into the wrong hands
- understand what systems are critical to business operations and the impact if they were taken down



Visuals used to support content

Step 2

Develop an incident response plan

- allows for protection of sensitive data during a security breach - it will help you determine the extent of the incident and manage the impact
- a good plan will draw on a range of organisational capabilities
- plan ahead - locating an incident response provider in the middle of an incident will delay response and recovery work
- test your plan regularly



Visuals used to support content

Step 3

Create a strong cyber security culture

- consider a cyber training course for employees
- raise awareness of common attacks and how they might present themselves within an organisation - phishing, ransomware, DDos, malware
- provide a process for reporting suspicious emails / potential attacks

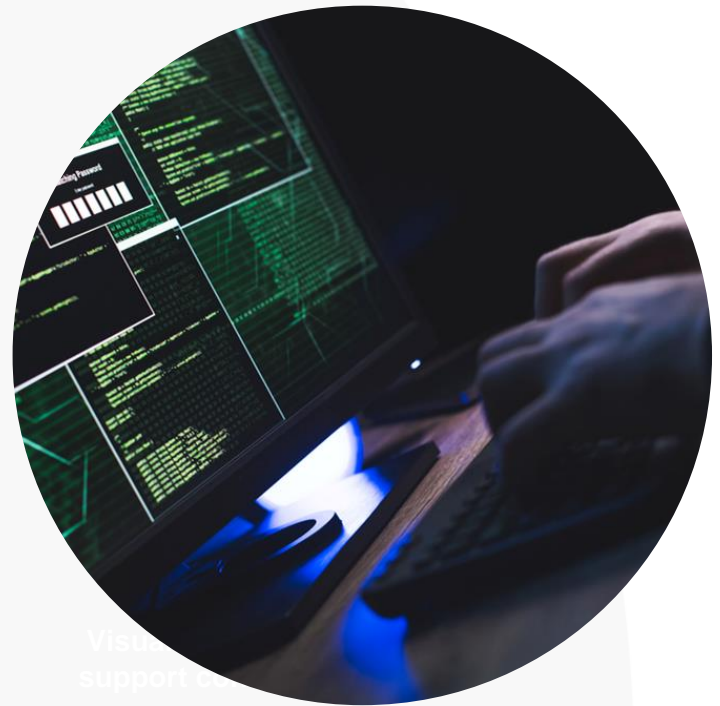


Visuals used to support content

Step 4

Keep up to date with emerging threats

- new types of malware are created every day
- increase resilience by learning about the ever changing threat landscape through relevant and credible sources
- adapt your protection and detection methods



Visit
support

Step 5

Develop a BC/DR Plan

- a business continuity/disaster recovery plan will help you recover from a disaster and resume critical/core business functions and operations
- similar to IR a good plan it will draw on a range of organisational capabilities
- test your plan regularly



Visuals used to support content

Procurement's role in cyber security

Power to your **procurement**



Crown
Commercial
Service

Procurement's role

- Crown Commercial Service partners with the National Cyber Security Centre (NCSC) to ensure agreements include appropriate security standards and assurances, such as Cyber Essentials
- The Cyber Security Services 3 agreement includes NCSC assured services to improve your security function, assessed to meet the NCSC's high quality standards



Describe your
image



Power to your procurement

Keep in touch

crowncommercial.gov.uk/cybersecurity

cybercategory@crowncommercial.gov.uk



@gov_procurement



Crown Commercial Service



Crown
Commercial
Service