The National Cyber Security Centre
Incident Management
Peter Yapp, Deputy Director Incident Management
What is the NCSC

The new National Cyber Security Centre is the UK’s authority on cyber security and part of GCHQ.

The NCSC brings together cyber security into a single, expert organisation building on the best of what we already have and combining the functions of:

• CESG
• CERT-UK
• Cyber related aspects of Centre for the Protection of National Infrastructure
• Centre for Cyber Assessment (CCA)
Our Vision
Helping to make the UK the safest place to live and do business online

What we do

• Reduce the cyber security risk to the UK
• Respond effectively to cyber security incidents
• Understand the UK’s cyber security environment, sharing knowledge, addressing systemic vulnerabilities
• Nurture the UK's cyber security capability, providing leadership on key national cyber security issues
Our Organisation
A significant incident or threat requiring coordinated cross-government response. The response is likely to require activity from a number of government and private sector entities including direct victim engagement, wider mitigation activity, investigative and disruptive activity, cross government communication and public media handling.

The incident does not require formalised ongoing multiagency coordination. At the higher end, this may include state sponsored network intrusion, an incident which is part of a criminal campaign for financial gain, or the large scale posting of personal employee information.

National Emergency - an incident or threat which is causing or may cause serious damage to human welfare (including loss or disruption of critical systems) or serious and sustained strategic impact (economic cost, loss of data or reputational impact to the UK). Characterised by Real World Impact; citizens losing access to bank accounts on a national scale, power outage affecting a UK region.
The cyber threat: are you a target?

Cyber breaches and attacks over the past year:
• 65% of large firms
• 1 in 4 of all businesses

What is at risk?
• Your money
• Your data (e.g. customer details, intellectual property, confidential emails)
• Your day-today operations (e.g. customer website, internal systems)
• Your business’ reputation
Proportions of incidents reported last year

- Malicious Code: 30%
- Investigation: 13%
- Improper usage: 15%
- Denial of Service: 13%
- Unauthorised Access: 18%
- Scans/Probes: 11%
Not just a problem for the IT department

Will require a response from staff across teams:

- Legal
- HR
- Communications/Media
- C-level staff
- Business Continuity
Cyber-security Information Sharing Partnership (CiSP)

- CiSP is a joint government and industry initiative to share cyber threat information, hosted by NCSC
- Free to join – funded by UK government
- Current membership stands at just shy of 7000 individuals and over 2500 organisations
- The ‘Fusion Cell’ stimulates discussion and sharing on the platform and provides all source assessment
- Sharing is based on Traffic Light Protocol
- CiSP produces a range of products/outputs including alerts and analysis papers for organisations