Alert: NCSC advises UK organisations to take action following conflict in the Middle East

In response to the evolving events in the Middle East, the NCSC is advising that UK organisations review their cyber security posture.

How has the cyber threat changed?

- As a result of the ongoing conflict in the Middle East, there is likely no current significant change in the direct cyber threat from Iran to the UK, however due to the fast-evolving nature of the conflict, this assessment may be subject to change.

- There is almost certainly a heightened risk of indirect cyber threat for those organisations and entities who have a presence, or supply chains, in the Middle East.

- Iranian state and Iran-linked cyber actors almost certainly currently maintain at least some capability to conduct cyber activity.

How should organisations respond?

- Organisations should prepare to respond to the risk of collateral impacts in the UK from Iran-linked hacktivists by reading previously issued advisories on **DDoS attacks**, **phishing activity** and **ICS Targeting**.

- For organisations exposed to higher risk, for example with those with offices or supply chains in the region, you should adjust your cyber security posture accordingly. You should take the steps outlined in our **actions to take when threat is heightened guidance**, and consider proportionate action to **increase monitoring** and **review your external attack surface**.

- The NCSC continues to encourage UK organisations to sign up to its **Early Warning service**, to receive timely notifications of security issues affecting their networks.

- In addition, given this is an evolving situation, CNI organisations may wish to pre-emptively review the NCSC's recently published guidance on **actions to take now to prepare CNI organisations for severe cyber threat**.

- For physical and personnel security risks, please refer to **guidance** issued by the National Protective Security Authority (NPSA). In particular following the **sabotage guidance** will help you protect your site from physical threats.

Review your organisation's risk posture, take proportionate action and report any concerns

Organisations are advised to review their risk posture, take proportionate action and report any concerning activity to the NCSC's Incident Management team using Report a cyber incident.

Report a cyber incident

PUBLISHED

2 March 2026

WRITTEN FOR

Cyber security professionals Large organisations Public sector

NEWS TYPE

Alert