Disruptive cyber activity highlights risk from internet-exposed systems and edge devices

Targeting of operational technology reinforces the need for organisations to understand what is exposed to the internet, address avoidable vulnerabilities, and build long-term cyber resilience.

What has happened?

The NCSC has seen increased targeting of operational technology (OT) systems across multiple sectors globally, including in the UK. This has been carried out by a range of threat actors and resulted in some limited real-world disruption.

Any organisation that uses, deploys or maintains OT systems should treat this development seriously and review their security posture accordingly.

Who is affected?

Any organisation with internet-exposed OT could be affected by this activity.

Organisations should not assume that their OT is inaccessible from the internet without verifying it, as unintended exposure can arise through misconfigurations, legacy connections, or unmanaged assets.

Wider context

The NCSC has been engaging with sectors directly in response to this recent targeting and is now sharing this advisory to support national resilience efforts.

For some time, the NCSC has been warning about a broader pattern of disruptive cyber activity carried out by state and non-state actors affecting organisations in both critical national infrastructure (CNI) and non-CNI sectors.

Against the backdrop of technology-enabled uplifts in cyber capability and increased geopolitical instability, the NCSC assesses that the threat from state use of offensive cyber, including outside of conflict, has almost certainly increased.

As a result of this wider context, it is essential that all organisations take action now given the developing threat picture.

What should I do?

In response to the observed disruptive activity, organisations should take the following actions:

+ Show All

1. Build a definitive view of your OT assets and ensure OT devices are not directly accessible from the public internet

+ Show

Build a definitive view of your OT architecture, including all assets, communications pathways and external connections. This will help identify internet-exposed systems, unmanaged assets and legacy connectivity that may introduce risk. Ensure OT devices, such as Programmable Logic Controllers (PLCs) and Human Machine Interfaces (HMIs), are not directly exposed to the public internet.

2. Replace default credentials and strengthen access controls for OT systems

+ Show

Change default credentials and prevent the use of shared passwords on web interfaces, management interfaces, and management protocols. Use unique accounts for administrators, enable multi-factor authentication (MFA) wherever supported, and use stronger authentication mechanisms such as public/private key authentication if supported by protocols (eg SSH) instead of passwords where possible.

3. Control access to OT networks and maintain secure, supported boundary devices

+ Show

Harden your OT boundary. Strictly control access to OT from external or untrusted networks. Ensure devices (such as industrial gateways, firewalls, routers and remote access appliances) that facilitate external connectivity are within vendor support, routinely updated by default, replaced before they reach their end-of-life (EOL), and that the management of these devices is only possible from a segregated management network that is not connected to the internet.

4. Adopt secure industrial and management protocols wherever possible

+ Show

Adopt secure versions of industrial and management protocols where possible. For industrial protocols this might mean migrating DNP3 to DNP3-SAv5, CIP to CIP Security, Modbus to Modbus Security, OPC DA to OPC UA. In management this includes but is not limited to removing the use of, telnet, SNMP v1, SNMP v2. Limit use of insecure protocols (where there is no secure alternative) to isolated network segments.

5. Ensure all connectivity to and within OT networks is logged and monitored

+ Show

Log and monitor all connectivity to and within OT networks, with particular focus on detecting attempts to communicate with OT assets such as PLCs and HMIs from unexpected devices, networks, or routes. As OT environments are typically static and predictable, baseline monitoring can be highly effective at identifying unauthorised activity, misconfigurations, or potential cyber compromise.

6. Ensure OT devices are operated in a state that prevents remote programming during normal operations

+ Show

There are multiple ways to achieve this such as ensuring PLCs are not left in PROGRAM or other maintenance modes. You should also ensure controller logic uses password-based write protection or equivalent mechanisms to prevent unauthorised changes to control logic from malicious endpoints. This reduces the risk of accidental modification and make it more difficult for malicious software or threat actors to alter operational processes.

7. Separate OT, management and business networks to limit the impact of incidents

+ Show

Segment management networks, OT control systems, and business IT networks to reduce the impact of a cyber incident. Separate systems based on their function and criticality and restrict communications between network zones to only those required for operational purposes. This helps prevent unauthorised access, limits opportunities for an attacker to move between systems, and reduces the likelihood that a compromise in one area will affect the wider environment.

8. Maintain tested backups and recovery procedures for critical OT systems

+ Show

Maintain tested backups of OT systems, configurations, controller logic, and critical engineering data, and regularly practise restoration and recovery procedures. Ensure you can quickly isolate affected systems from the wider network and restore essential operations from trusted backups to minimise downtime and support safe recovery from cyber incidents. Backups should be designed to be ransomware-resistant.

Implications for non-operational technology organisations

While we have observed targeting of OT, there continues to be a broader pattern of disruptive cyber activity targeting internet exposed systems and edge devices affecting all sectors

We have previously highlighted other activity such as that against poorly configured routers, published in July 2026 with international partners.

For non-OT organisations, such activity highlights the importance of maintaining visibility of internet-exposed assets and edge network devices. Key actions include maintaining an accurate inventory of internet-facing systems, understanding the function and data flows of edge devices, applying vendor security updates promptly, retiring end-of-life equipment, disabling insecure management protocols such as SNMP v1, SNMP v2 and Telnet, and monitoring for unexpected configuration changes or outbound connections.

Building long-term cyber resilience

Effective cyber resilience requires organisations to be prepared before an incident occurs and capable of responding and recovering when one does.

Organisations should review their readiness for significant cyber incidents, taking account of the NCSC's guidance on preparing for severe cyber threats, and ensure that arrangements for responding to and recovering from cyber attacks are established, maintained and regularly exercised in line with the NCSC's guidance on what to do when cyber attacks disrupt your organisation.

All organisations should register for the NCSC's free Early Warning service to help identify publicly exposed vulnerabilities and other potential security issues affecting internet-facing systems, supporting efforts to detect and address risks before they are exploited.

Cyber Assessment Framework

Organisations that have embedded strong cyber resilience practices are better placed to prevent, detect and respond to cyber incidents before they cause operational disruption.

The Cyber Assessment Framework (CAF) provides a comprehensive framework for assessing how well an organisation is meeting expected security and resilience outcomes. Boards should seek assurance that the outcomes and principles described within the CAF are being achieved across all systems supporting essential functions.

Cyber Essentials

Where the CAF is not appropriate, Cyber Essentials is an excellent first step in gaining assurance that your systems are protected against the most common threats. It is the minimum standard of cyber security recommended by the Government for organisations of all sizes.

Further resources

- What to do when cyber attacks disrupt your organisation | NCSC
- Early Warning | NCSC
- Secure connectivity principles for Operational Technology | NCSC
- Operational Technology: Secure connectivity - Water Sector Example | National Cyber Security Centre | NCSC
- Operational Technology: Creating and maintaining a definitive view of your OT architecture | NCSC

- Primary Mitigations to Reduce Cyber Threats to Operational Technology | CISA
- Internet Exposure Reduction Guidance | CISA
- Vulnerability management | NCSC
- Cyber Assessment Framework | NCSC

PUBLISHED

27 August 2026

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

NEWS TYPE

Alert