PROTECTING WHAT MATTERS

Industrial Control Systems

Most of the UK's essential services now rely on Industrial Control Systems (ICS) for delivery and operation. These sytems can be connected via the internet and controlled remotely.

Infrastructure relies on Industrial Control Systems

WATER

Each person in the UK uses about 150l of water a day

OIL

The UK consumes 1.217m barrels of oil per day

GAS

The gas we extract from under the sea heats about 80% of British homes

ELECTRICITY

The UK was powered up via 29.9m electricity meters in 2013

TRANSPORT

Every day there are 24m journeys made across public transport in London

CIVIL NUCLEAR

Nuclear energy currently supplies 20% of the UK's electricity

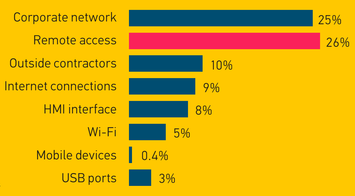
CHEMICALS

The UK's chemical industry supports half a million jobs

But enabling connectivity and remote access on this scale introduces vulnerabilities

Did you know that the average ICS has 11 different connections?[1]
Monitoring these is key to understanding the risks.

Malicious code is getting onto our industrial networks in different ways

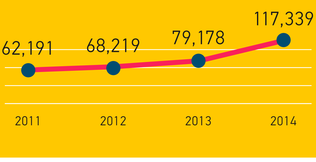


Cyber attacks are on the rise[2]

Annual global cost:

£400 BILLION

Number of cyber attacks to UK businesses per day



And Industrial Control Systems are being targeted

Stuxnet was the first known autonomous threat to target and sabotage Industrial Control Systems to such an extent

The target is believed to be a uranium enrichment facility

Infected the software of at least

14 INDUSTRIAL SITES

LNK and PIF files allowed the threat to auto-execute onto USB drives. The files were then spread to systems not connected to the internet

This meant that there were other un-targeted systems that were also infected

40,000 infected IP addresses

155 countries

In 2003 the Slammer worm infected the security system of a nuclear power plant

Introduced by a private contractor's laptop

Safety monitoring was disabled for 5 hours

Fortunately the system was down for maintenance

How can you manage the risk?

CPNI have developed a framework and good practice guide for securing ICS. This comprises eight core elements that address the increasing use of standard IT technologies in ICS. You can use these as points of reference to help you develop and tailor ICS security, appropriate to the needs of your organisation.

- Establish ongoing governance
- Manage the business risk
- Manage Industrial Control Systems lifecycles
- Improve awareness and skills
- Select and implement security controls
- Manage vulnerabilities
- Manage third party risks
- Establish response capabilities

The framework and its supporting elements are intended to be a point of reference for an organisation to begin to develop and tailor ICS security that is appropriate to its needs

The Centre for the Protection of National Infrastructure protects national security by providing integrated protective security advice. For further advice on cyber security visit the CPNI website.

CPNI
Centre for the Protection of National Infrastructure

REFERENCES

1 Securing Critical Information Infrastructure: Trusted Computing Base: Securelist October 2012

2 Net Losses: Estimating the Global Cost of Cybercrime, McAfee, June 2014