DNV

The Energy Cyber Priority

The state of cyber security in the energy industry-sneak preview on latest research

Shaun Reardon; Head of section, industrial systems cyber security

11 May 2023

Cyber risks are evolving
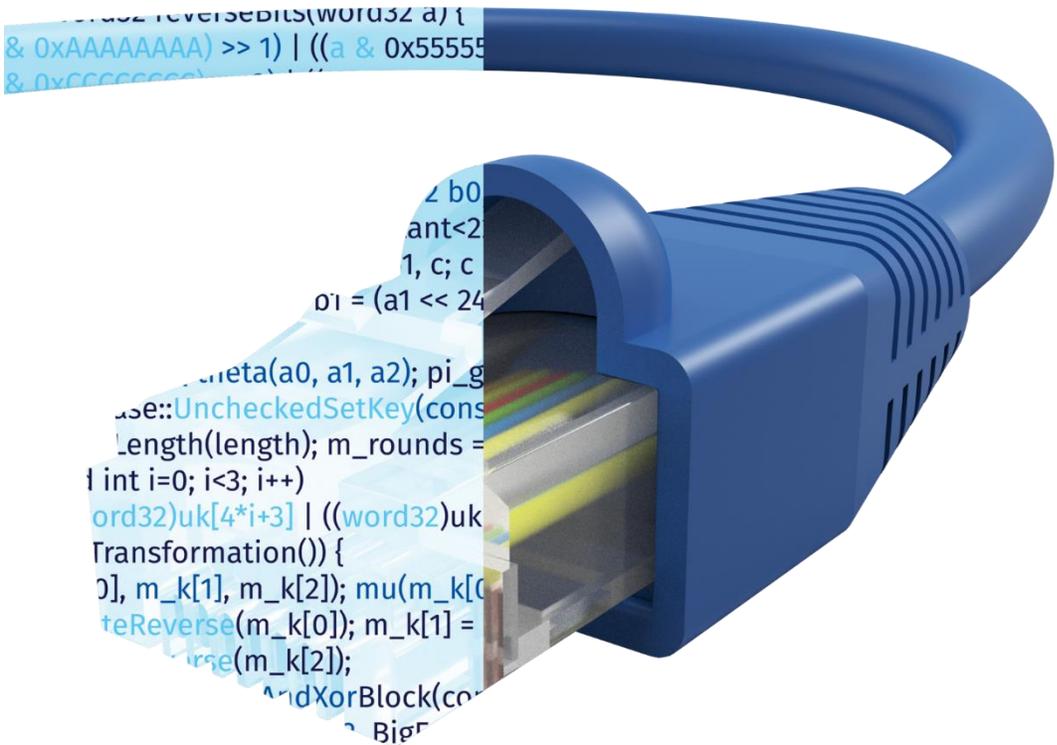
The energy sector now appears among the top three industries reporting cyber attacks

The sector has been tackling IT security for decades

Securing operational technologies is a more recent and urgent challenge

Operational technologies are becoming more networked and connected to IT

This opens the back door for hackers to access and take control of critical infrastructure.

DNV

Sneak preview into our research

- How real is the industry's awareness of the threat?

- What action is being taken to prevent it?

- Where is investment being prioritized?

|		
601 Energy professionals surveyed	**92** Countries represented	**59%** Support, develop or operate operational technology

In-depth analysis of our survey findings will be published in a new report 6th of June.

A step change in awareness

Energy professionals anticipate that their organization is more vulnerable to cyber-attacks on its OT environments today than it has been at any other time in its history
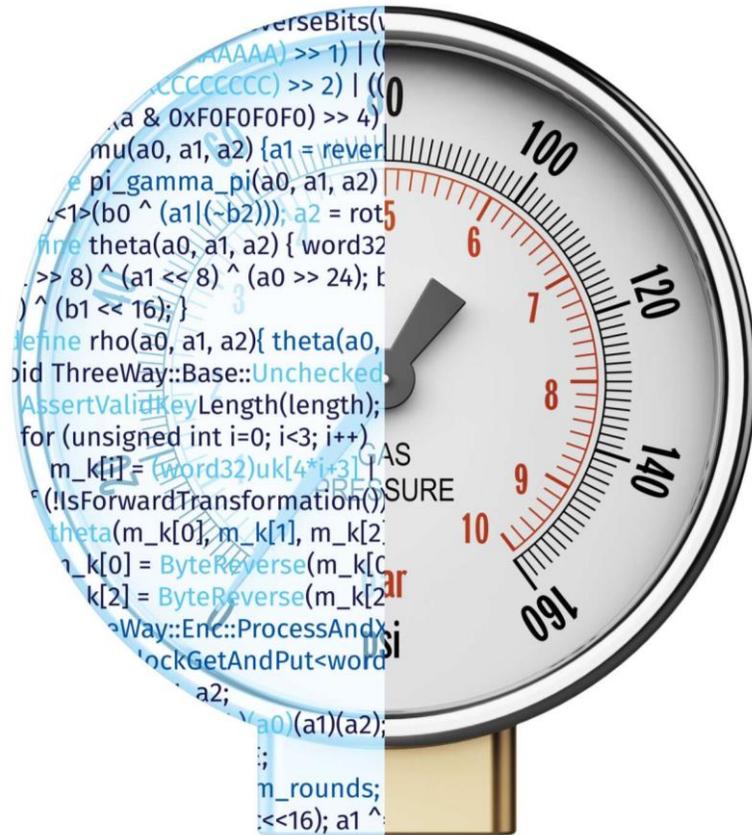
77%
Say geopolitical uncertainty has made their organization more aware of the potential vulnerabilities in the cyber security of their OT

64%
State their organization is more vulnerable to cyber-attacks on its OT environments today than it has been at any other time in its history

89%
of energy professionals believe cyber security is a pre-requisite for digital initiatives

59%
Say cyber security is a regular topic on the agenda for the organization's board of directors/senior management

DNV

Growing understanding of the risk

SECURITY BY DESIGN

54%
Say that they consider security at every stage of the lifecycle of their assets and infrastructure

69%
Tell us that cyber is a consideration during the early phases of new energy infrastructure projects

SUPPLY CHAIN SECURITY

among top **5**
Challenges companies face strengthen OT cyber defences

57%
Say their organisation has good oversight of supply chain vulnerabilities

SAFETY AND BUSINESS RISK

71%
Tell us they take cyber security as seriously as physical health and safety

77%
Report that cyber security is now treated as a business risk

DNV

Industry faces challenges

42%

Say their organisation's current level of investment is sufficient to ensure the resilience oft heir operations and infrastructure

No. 1

Say lack of in-house cyber security is the single most important barrier to cyber maturity
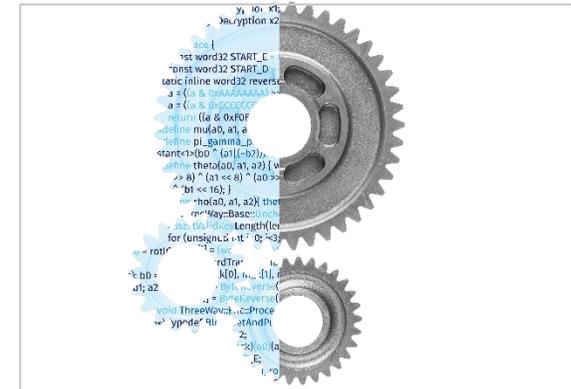
76%

Believe that cyber professionals need to get better at speaking the language of energy operations

DNV

Regulation leads drivers for investment

Driver	Percentage
Regulatory requirements	49%
A cyber incident or near-miss in my organization	38%
A cyber incident or near-miss impacting another organization in our sector	34%
Increased focus on cyber security from the leadership in my organization	29%
Pressure from customers	26%
Clearer assessment of our weaknesses and vulnerabilities	24%
Development of industry-specific solutions	20%

DNV

Thank you!
dnv.com/cybersecurity

DNV