The State of Industrial Cybersecurity in Belux - Q1 21

iVOX 20200429

TREND MICRO™

iVOX
We spark connections

The State of Industrial Cybersecurity in Belux - Q1 21

iVOX 20200429

TREND MICRO™

iVOX
We spark connections

Study design

Purpose of the study

- Brief survey on cybersecurity in industrial cybersecurity in the Belux

Target group

- Belgians working in companies with more than 500 employees, who have decision-making authority over, influence on or at least good insight into decisions relating to industrial control systems and IT systems in their company
- Focus on employees within production companies, logistics & transport, maritime, rail and aviation industries and oil, gas and chemical industries
- Focus on employees from IT and operational departments (production, maintenance, etc.)
- Focus on individuals in a management position

Method

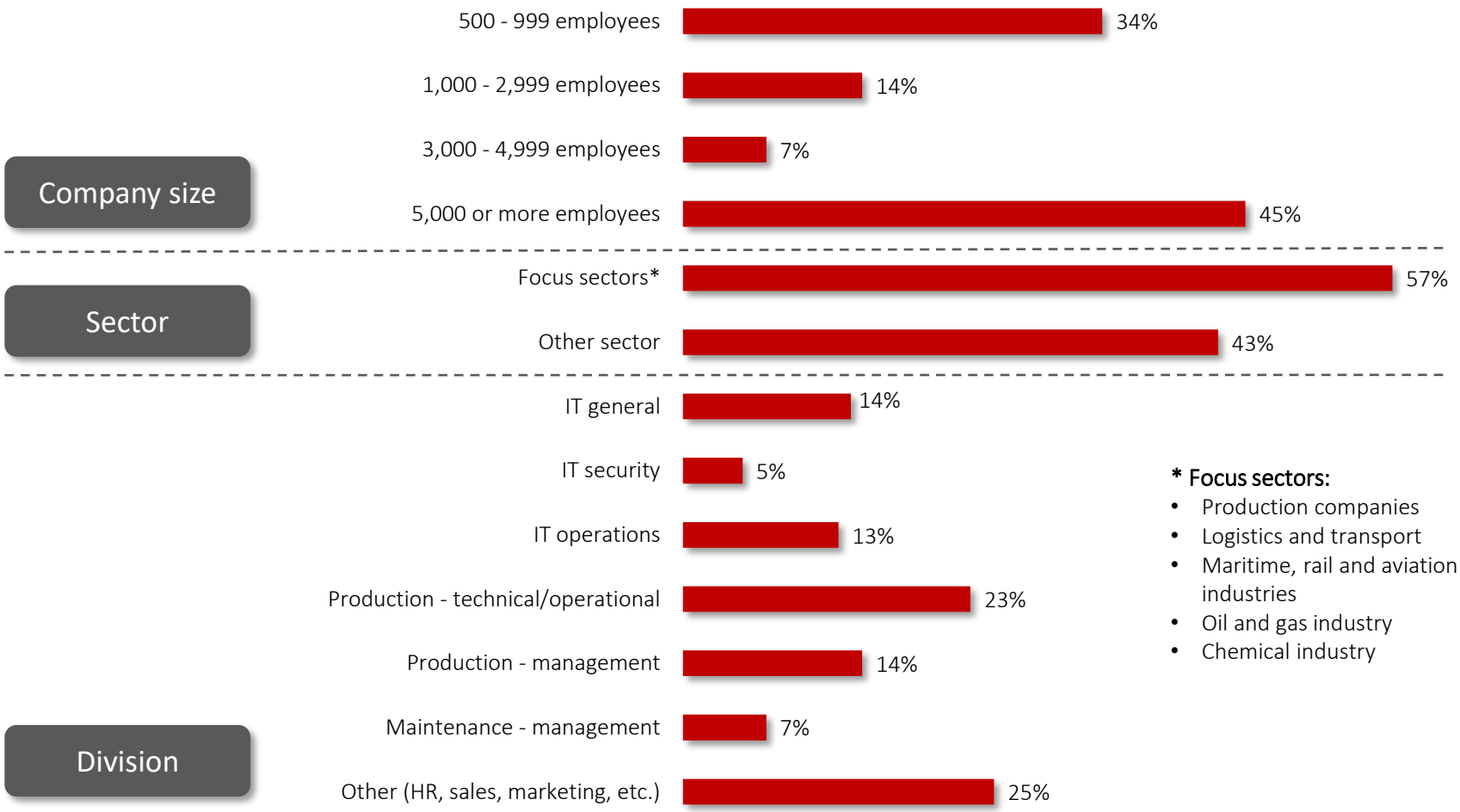
- Field work mainly carried out on the iVOX online survey panel (n=96) and partly on the database of Trend Micro itself (n=8)
- Field work: from 19/11/2020 to 8/3/2021
- N: 104
- Maximum margin of error with a sample of 104 respondents (95% confidence): 9.58%

Significant differences

- Significant differences (95% confidence interval) are indicated with  or 

Contents

Composition of sample



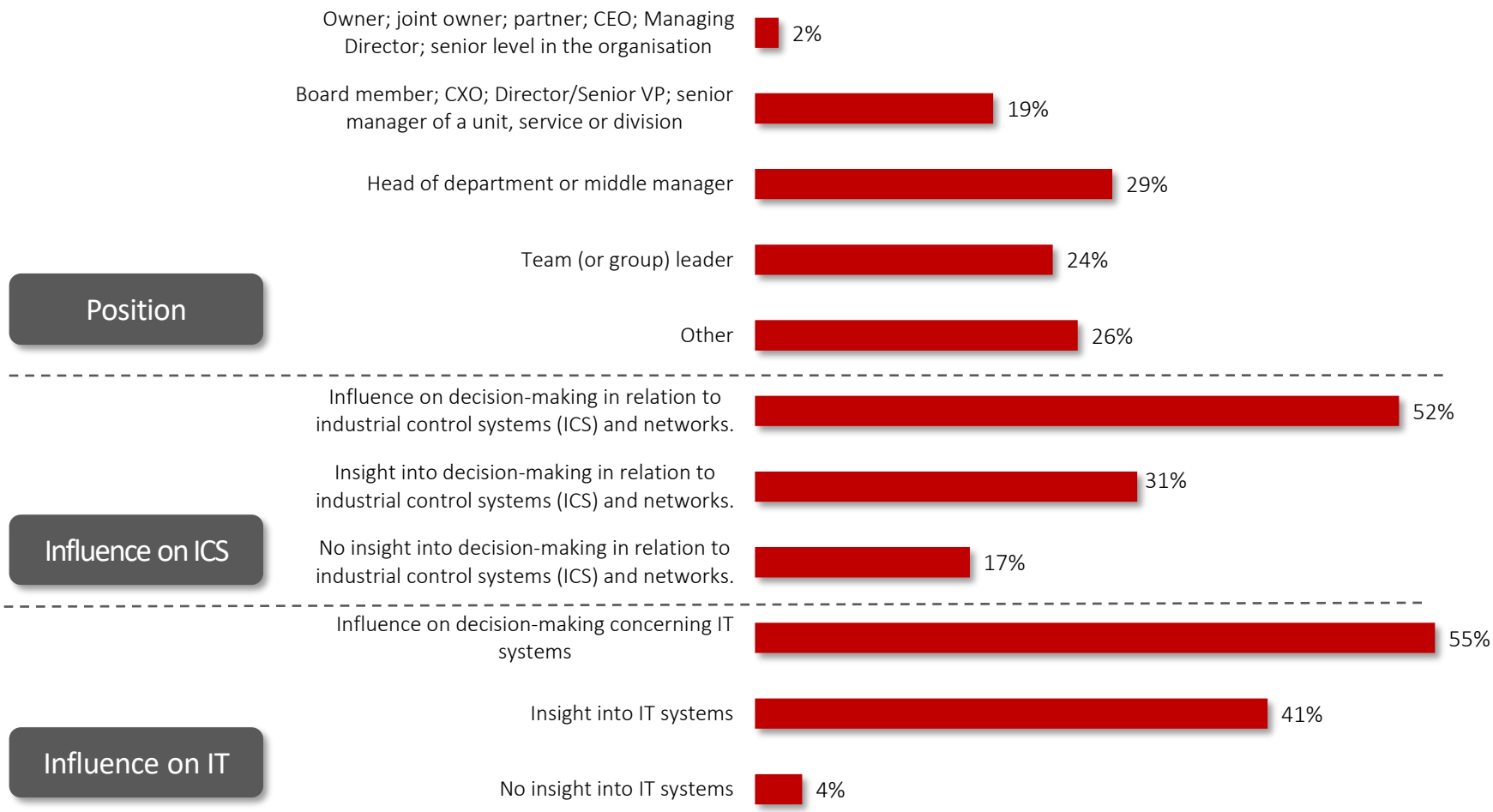
*** Focus sectors:**

- Production companies
- Logistics and transport
- Maritime, rail and aviation industries
- Oil and gas industry
- Chemical industry

Filter: none

N: 104

Composition of sample



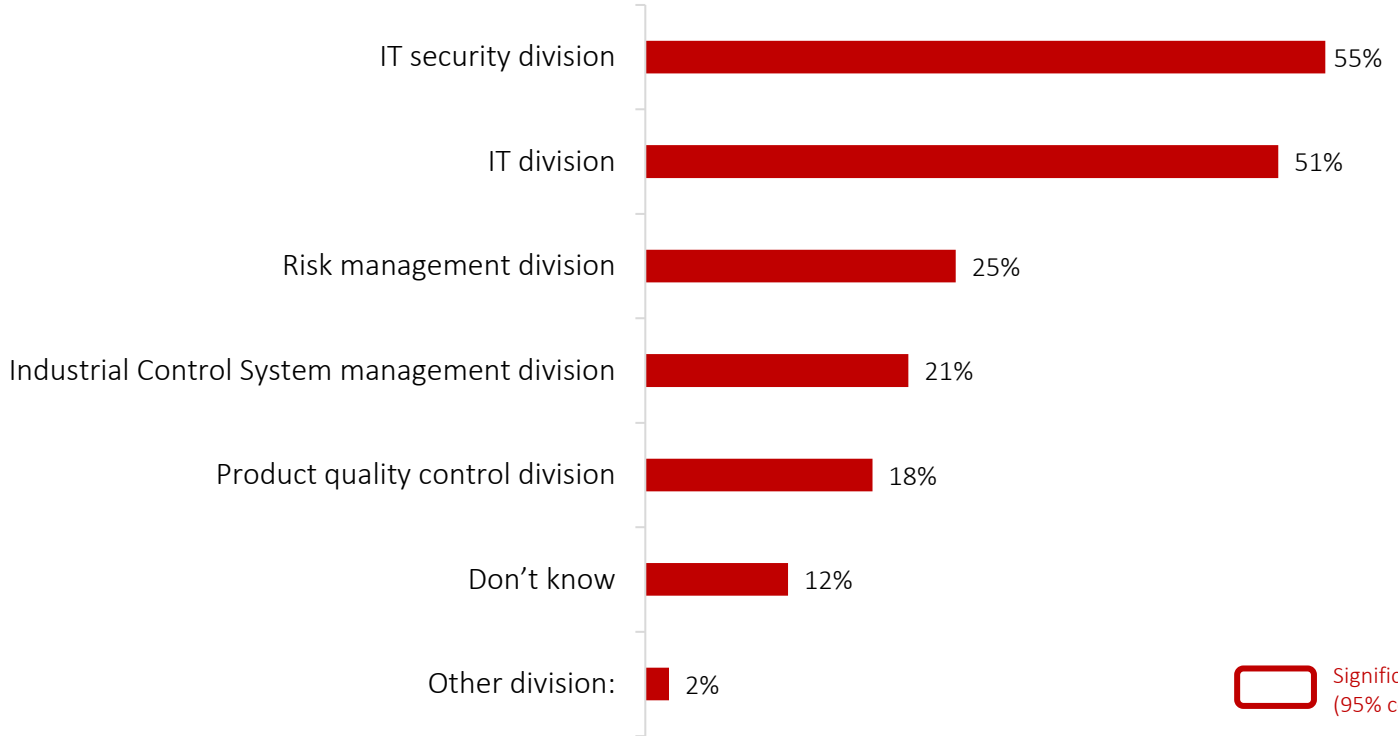
Filter: none

N: 104

Contents

It is mainly the IT security division and the IT division that are involved in decisions on technical measures in the area of cybersecurity.

When your organisation decides what technical measures should be used in the area of cybersecurity to secure smart factories, which of the following divisions are involved in decision-making?



Filter: none
N: 104

Respondents from larger companies more often state that the decision is made within the product quality control division.

When your organisation decides what technical measures should be used in the area of cybersecurity to secure smart factories, which of the following divisions are involved in decision-making?

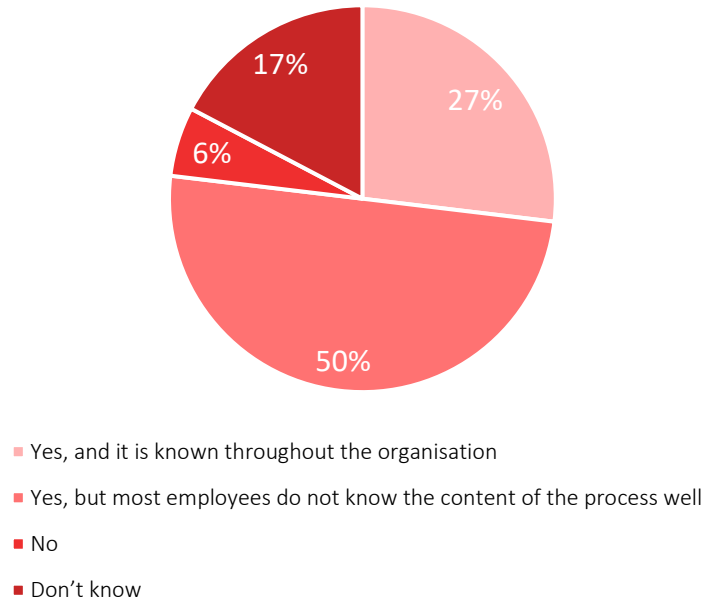
	total	Company size		sector: production companies, logistics & transport, maritime, rail and aviation, oil & gas, chemical		operating systems: final decision-maker, other decision-maker, influence on decision-making		IT: final decision-maker, other decision-maker, influence on decision-making	
		500 - 4,999 employees	5,000+ employees	No	Yes	No	Yes	No	Yes
IT security division	55%	49%	62%	49%	59%	52%	57%	51%	58%
IT division	51%	54%	47%	47%	54%	52%	50%	49%	53%
Risk management division	25%	19%	32%	29%	22%	26%	24%	28%	23%
Industrial Control System management division	21%	18%	26%	18%	24%	18%	24%	13%	28%
Product quality control division	18%	11%	27.7% B	13%	22%	16%	20%	17%	19%
Don't know	12%	12%	11%	16%	9%	18.0% B	6%	19.1% B	5%
Other division:	2%	2%	2%	4%	0%	4%	0%	2%	2%

Significantly higher (95% confidence)

Filter: none
N: 104

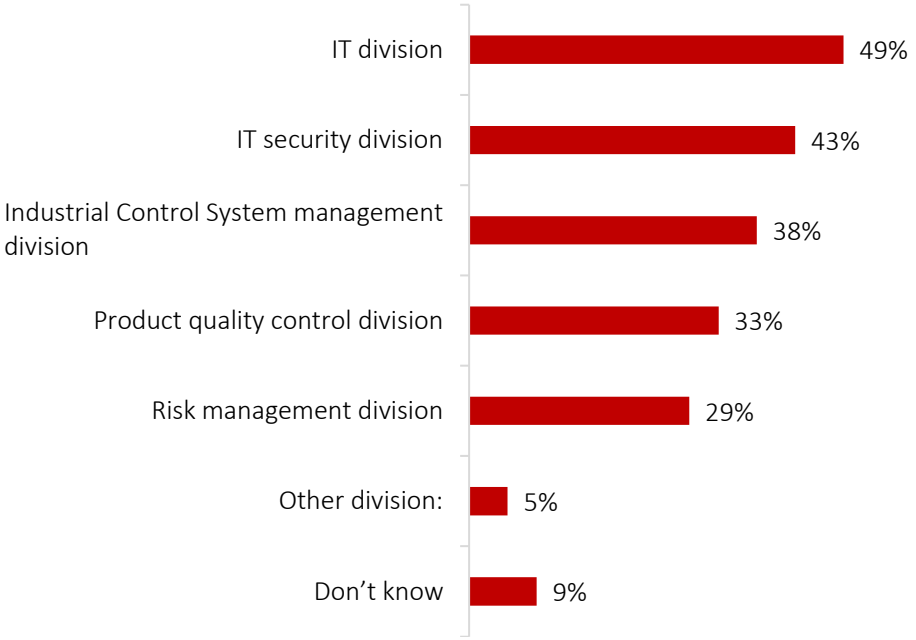
Most companies (77%) have created an operational process, but the employees do not know the process well.

Has your organisation created an operational process when deciding on cybersecurity measures?



Filter: none
N: 104

Which divisions are involved in making decisions on the operational process in smart factories within your organisation?



Filter: if the company has an operational process
N: 80

Respondents from focus sectors indicate in 84% of cases that an operational process has been created.

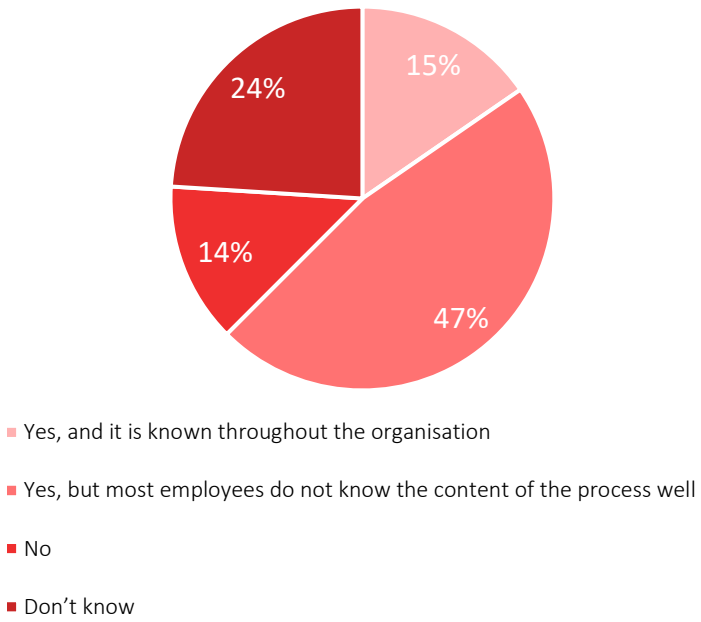
Has your organisation created an operational process when deciding on cybersecurity measures?

	total	Company size		sector: production companies, logistics & transport, maritime, rail and aviation, oil & gas, chemical		operating systems: final decision-maker, other decision-maker, influence on decision-making		IT: final decision-maker, other decision-maker, influence on decision-making	
		500 - 4,999 employees	5,000+ employees	No	Yes	No	Yes	No	Yes
Yes, and it is known throughout the organisation	**27%**	28%	26%	22%	31%	32%	22%	26%	28%
Yes, but most employees do not know the content of the process well	**50%**	54%	45%	47%	53%	44%	56%	47%	53%
No	**6%**	7%	4%	4%	7%	6%	6%	6%	5%
Don't know	**17%**	11%	25.5% B	26.7% B	10%	18%	17%	21%	14%

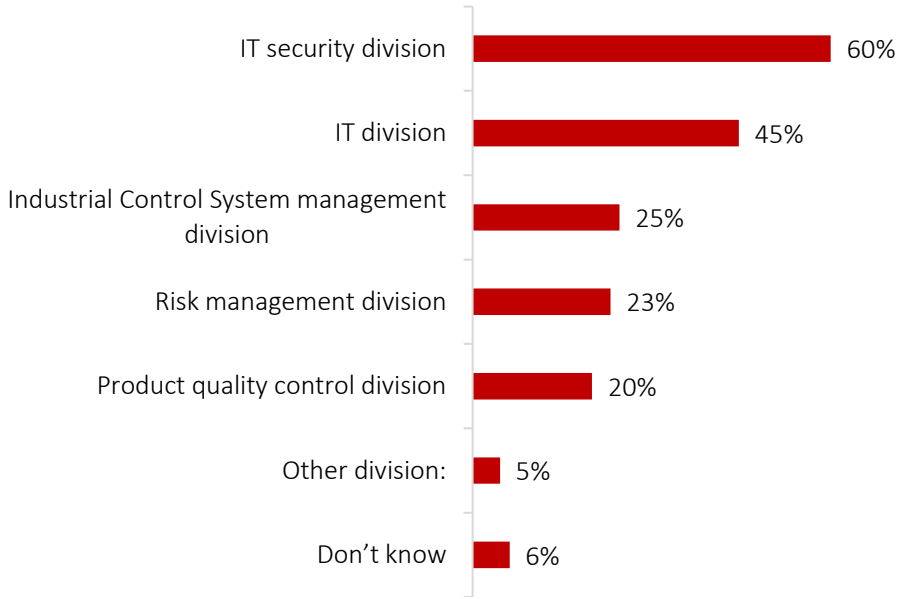
Filter: none
N: 104

2 out of 3 respondents state that a cyberincident response process has been developed, but once again the employees do not know the process well.

Has your organisation created a cyberincident response process when deciding on cybersecurity measures for smart factories?



Which divisions are involved in your organisation's cyberincident process?



Filter: if the company has an operational process
N: 65

Filter: none
N: 104

IT decision makers are more often aware of the cyberincident response process, but they estimate that most of their colleagues are not aware of its content.

Has your organisation created a cyberincident response process when deciding on cybersecurity measures for smart factories?

	total	Company size		sector: production companies, logistics & transport, maritime, rail and aviation, oil & gas, chemical		operating systems: final decision-maker, other decision-maker, influence on decision-making		IT: final decision-maker, other decision-maker, influence on decision-making	
		500 - 4,999 employees	5,000+ employees	No	Yes	No	Yes	No	Yes
Yes, and it is known throughout the organisation	**15%**	18%	13%	16%	15%	18%	13%	13%	18%
Yes, but most employees do not know the content of the process well	**47%**	49%	45%	38%	54%	46%	48%	34%	57.9% A
No	**14%**	16%	11%	16%	12%	8%	19%	19%	9%
Don't know	**24%**	18%	32%	31%	19%	28%	20%	34.0% B	16%

Filter: none
N: 104

Having a shared vision and insight into cybersecurity systems and technologies for production systems are seen as the top priorities when considering collaboration between the IT and/or IT security division and the industrial control system management division.

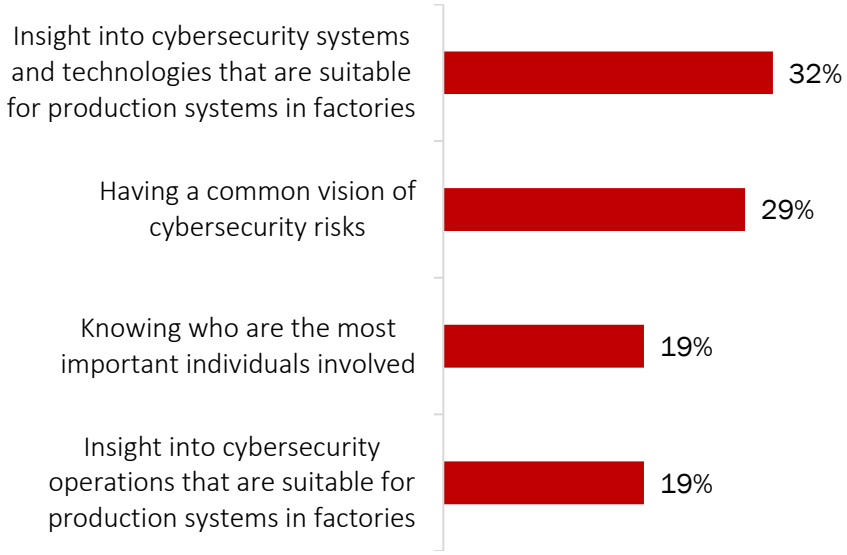
What is the top priority when considering collaboration between the IT and/or IT security division and the industrial control system management division?

Average ranking

1. Having a common vision of cybersecurity risks
2. Insight into cybersecurity systems and technologies that are suitable for production systems in factories
3. Insight into cybersecurity operations that are suitable for production systems in factories
4. Knowing who are the most important individuals involved

Significantly higher (95% confidence)

First place (top priority)

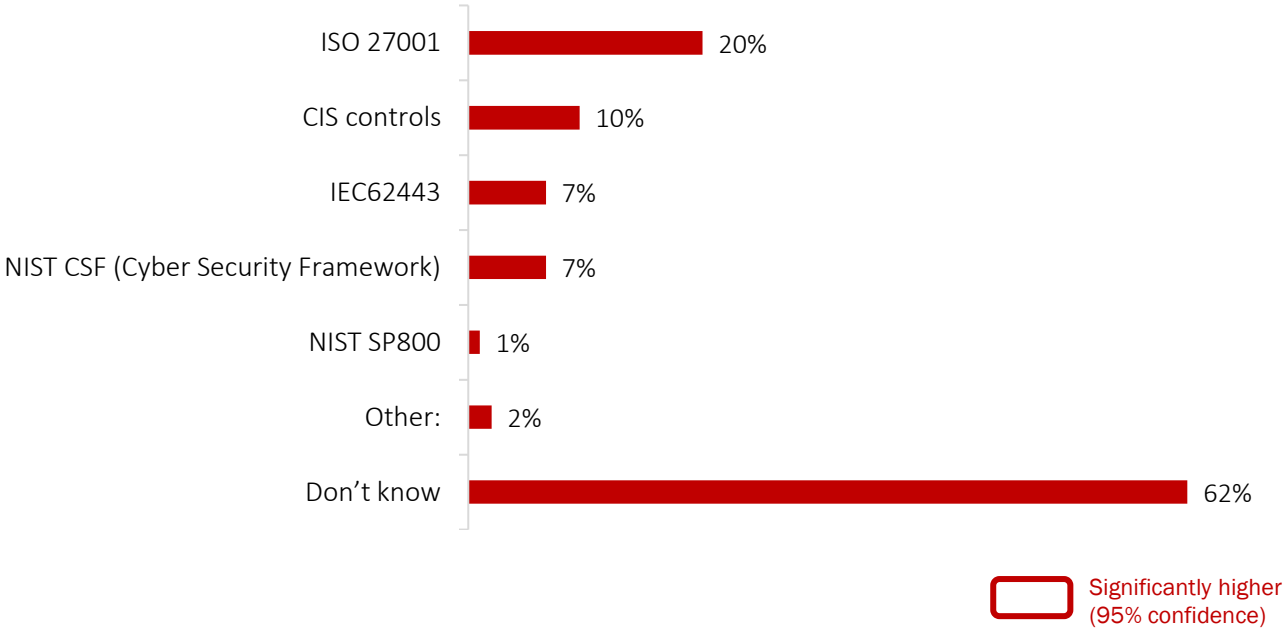


Filter: having no idea about these priorities

N: 75

A majority of the respondents do not know exactly what industrial standards their control systems should meet.

What regulations or industrial standards must your organisation's control systems meet?



Filter: none
N: 104

In half of cases, decision-makers at operational and IT levels also do not know this exactly.

What regulations or industrial standards must your organisation's control systems meet?

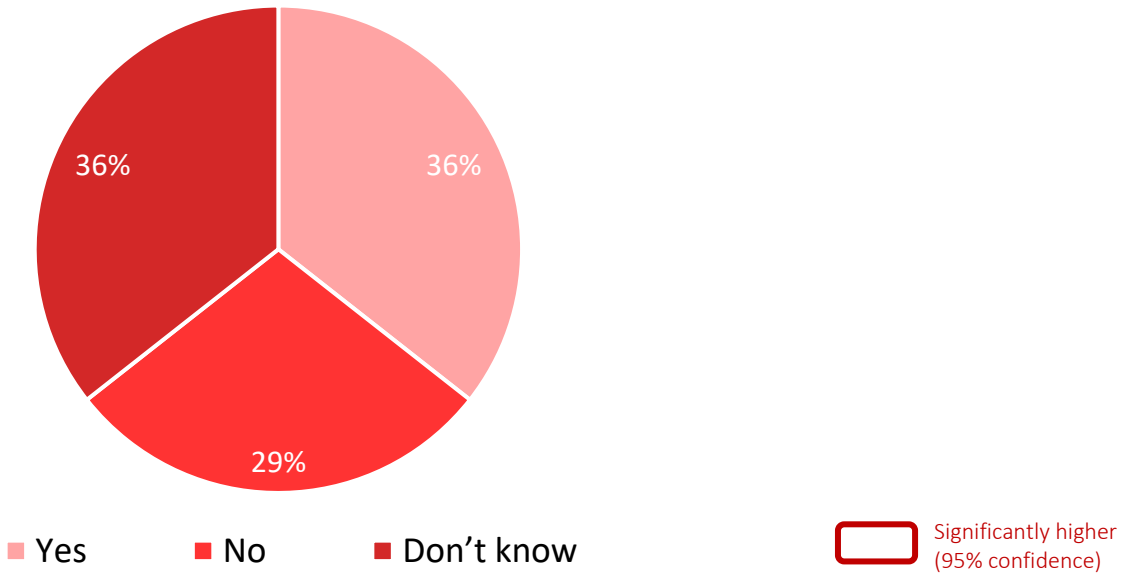
	total	Company size		sector: production companies, logistics & transport, maritime, rail and aviation, oil & gas, chemical		operating systems: final decision-maker, other decision-maker, influence on decision-making		IT: final decision-maker, other decision-maker, influence on decision-making	
		500 - 4,999 employees	5,000+ employees	No	Yes	No	Yes	No	Yes
ISO 27001	20%	21%	19%	18%	22%	22%	19%	23%	18%
CIS controls	10%	11%	9%	9%	10%	6%	13%	0%	18%
IEC62443	7%	11%	2%	4%	9%	2%	11%	0%	12%
NIST CSF (Cyber Security Framework)	7%	7%	6%	4%	9%	4%	9%	6%	7%
NIST SP800	1%	0%	2%	0%	2%	2%	0%	2%	0%
Don't know	62%	54%	70%	71%	54%	68%	56%	70%	54%
Other:	2%	4%	0%	2%	2%	4%	0%	2%	2%

Significantly higher (95% confidence)

Filter: none
N: 104

2 out of 5 respondents state that a protocol gateway has been installed in their factory network.

Do you have a protocol gateway installed in your factory network?



Filter: none
N: 104

In the survey's focus sectors, 46% of respondents state that a protocol gateway has been installed.

Do you have a protocol gateway installed in your factory network?

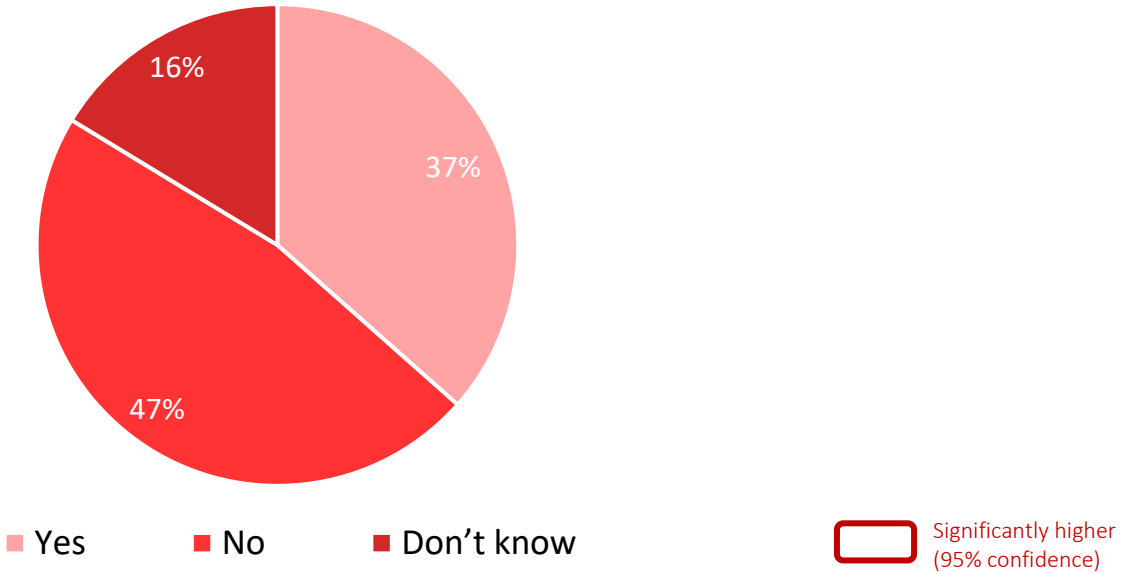
	total	Company size		sector: production companies, logistics & transport, maritime, rail and aviation, oil & gas, chemical		operating systems: final decision-maker, other decision-maker, influence on decision-making		IT: final decision-maker, other decision-maker, influence on decision-making	
		500 - 4,999 employees	5,000+ employees	No	Yes	No	Yes	No	Yes
Yes	**36%**	32%	40%	22%	45.8% A	32%	39%	30%	40%
No	**29%**	36.8% C	19%	31%	27%	30%	28%	28%	30%
Don't know	**36%**	32%	40%	46.7% B	27%	38%	33%	43%	30%

Significantly higher (95% confidence)

Filter: none
N: 104

2 out of 5 respondents state that their organisation has experienced a cyberincident in the past.

Has your organisation ever experienced a cybersecurity incident in your smart factories (for example, a computer virus, an unauthorised operation that exploits vulnerabilities in the system or unauthorised access to the system)?



Filter: none
N: 104

Respondents from smaller companies more often say that they have never experienced an incident.

Has your organisation ever experienced a cybersecurity incident in your smart factories (for example, a computer virus, an unauthorised operation that exploits vulnerabilities in the system or unauthorised access to the system)?

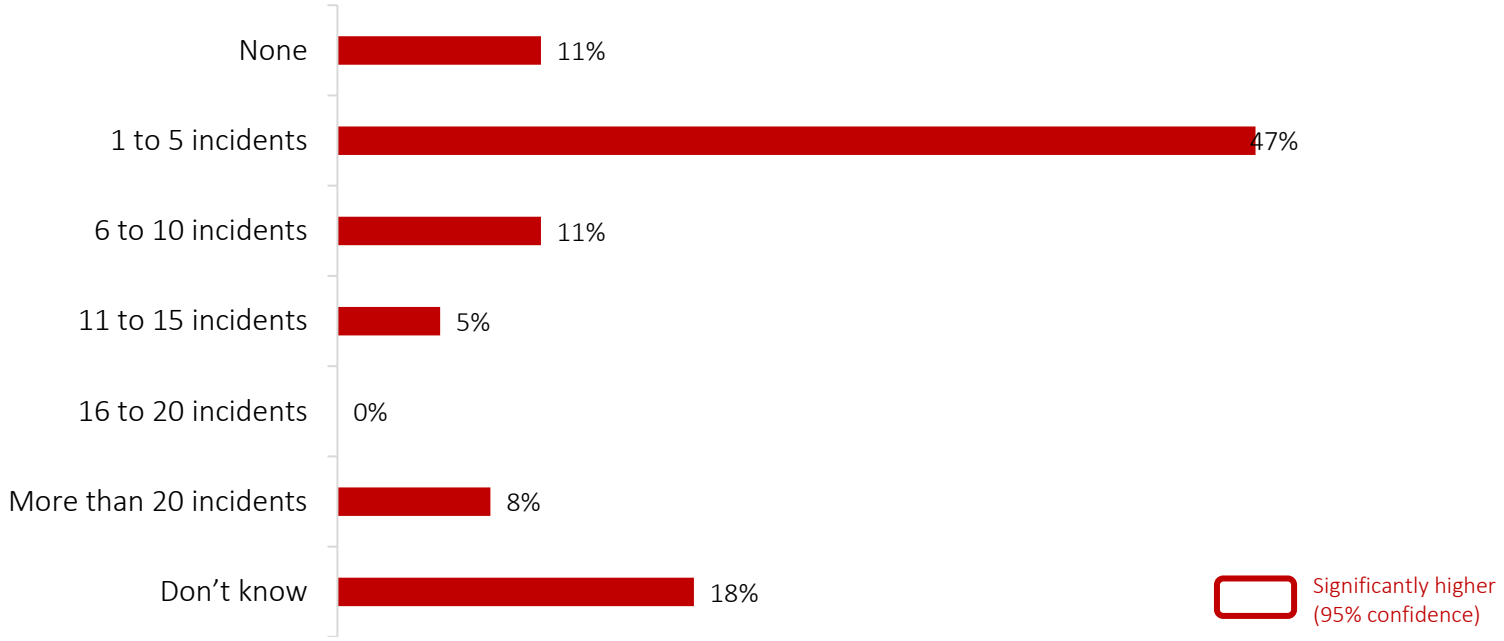
	total	Company size		sector: production companies, logistics & transport, maritime, rail and aviation, oil & gas, chemical	
		500 - 4,999 employees	5,000+ employees	No	Yes
Yes	**37%**	30%	45%	33%	39%
No	**47%**	56.1% C	36%	40%	53%
Don't know	**16%**	14%	19%	26.7% B	9%

Significantly higher (95% confidence)

Filter: none
N: 104

A total of 71% of those who have experienced an incident (=26% of all respondents) say that this occurred in the past 12 months.

How many cybersecurity incidents have there been in the past 12 months in all the smart factories in your organisation?



Filter: if a cybersecurity incident has occurred

N: 38 * warning: low basis

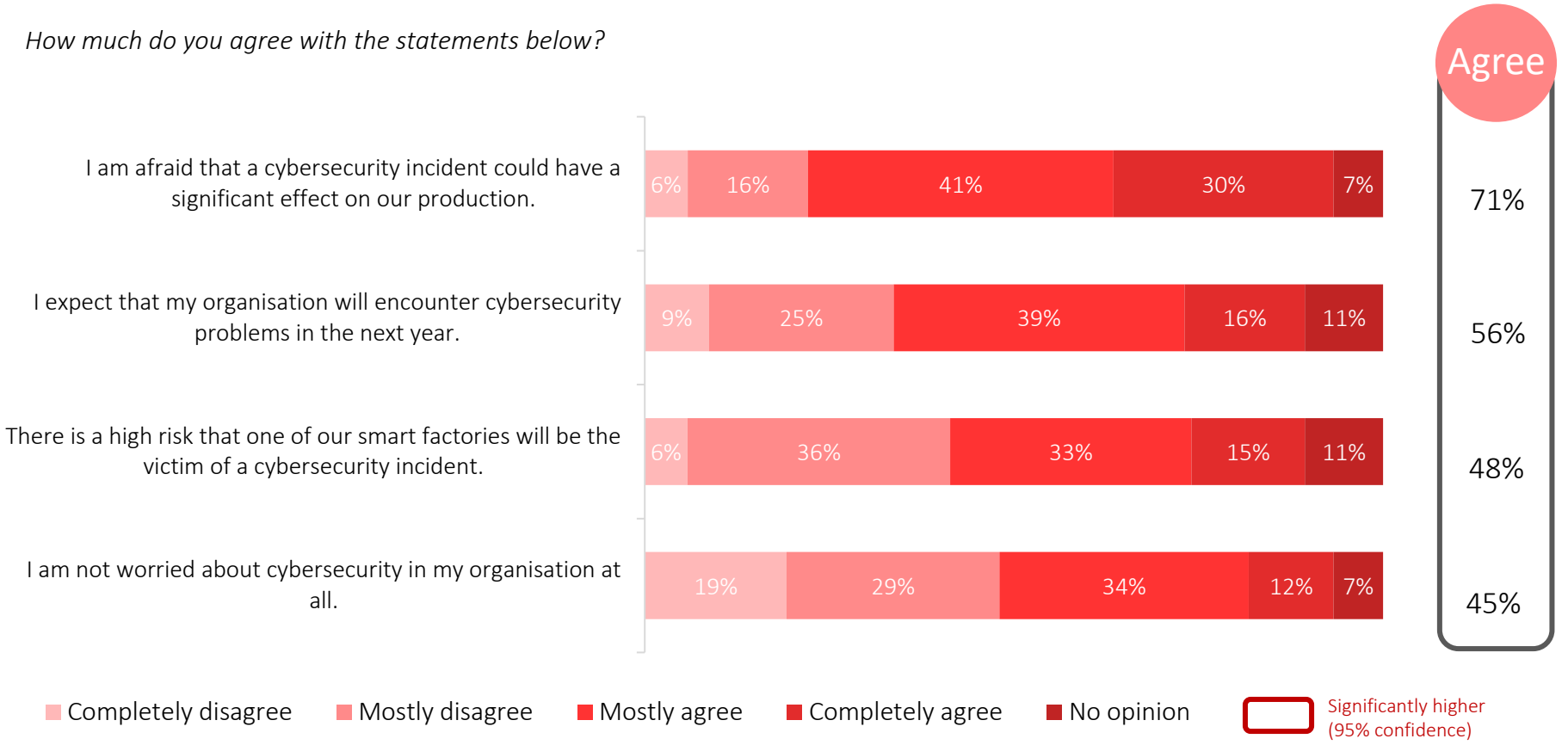
For 8% of those who have experienced an incident in the past (=3% of all respondents), the incident stopped the production systems.

Did these incidents stop the production systems in the smart factories in your organisation?

Filter: if a cybersecurity incident has occurred
N: 38 * warning: low basis

Most respondents are seriously concerned about cybersecurity incidents in their smart factories. A majority are expecting to encounter cybersecurity problems in the next year.

How much do you agree with the statements below?



Filter: none
N: 104

Mostly respondents who are decision-makers in relation to control systems are concerned about cybersecurity incidents in the (near) future.

How much do you agree with the statements below?

		total	Company size		sector: production companies, logistics & transport, maritime, rail and aviation, oil & gas, chemical		operating systems: final decision-maker, other decision-maker, influence on decision-making		IT: final decision-maker, other decision-maker, influence on decision-making	
			500 - 4,999 employees	5,000+ employees	No	Yes	No	Yes	No	Yes
There is a high risk that one of our smart factories will be the victim of a cybersecurity incident.	Agree	**48%**	42%	55%	53%	44%	34%	61.1% A	40%	54%
I am afraid that a cybersecurity incident could have a significant effect on our production.	Agree	**71%**	70%	72%	64%	76%	60%	81.5% A	55%	84.2% A
I am not worried about cybersecurity in my organisation at all.	Agree	**45%**	47%	43%	57.8% B	36%	42%	48%	47%	44%
I expect that my organisation will encounter cybersecurity problems in the next year.	Agree	**56%**	54%	57%	60%	53%	42%	68.5% A	49%	61%

Filter: none
N: 104

Significantly higher (95% confidence)

Contents

Key facts

1

- Most respondents state that their company has created an **operational process** and a **cyberincident response process** when deciding on its cybersecurity measures, but the employees are not sufficiently aware of their content.
- Having a **shared vision** and **insight into cybersecurity systems and technologies for production systems** are seen as the top priorities when considering collaboration between the IT and/or IT security division and the industrial control system management division.
- Two out of five respondents (almost half of the respondents from focus sectors) state that **a protocol gateway** has been installed in their factory network.

2

- Two out of five respondents state that their company has experienced a cyberincident in the past. According to one in four of them this happened in the past year.
- In 8% of cases it stopped the production systems.

3

- A majority of respondents, and certainly of decision-makers in relation to IT and control systems, are worried about cybersecurity incidents in the future.
  - ❑ A total of 71% are afraid that this type of incident could have a significant effect on their production
  - ❑ In addition, 56% expect that their company will encounter this during the coming year
  - ❑ Finally, 48% assess the risk of a cyberincident in their smart factories as “very high”.