Capgemini
RESEARCH INSTITUTE

built to defend

SMART & SECURE: WHY SMART FACTORIES NEED TO PRIORITIZE CYBERSECURITY

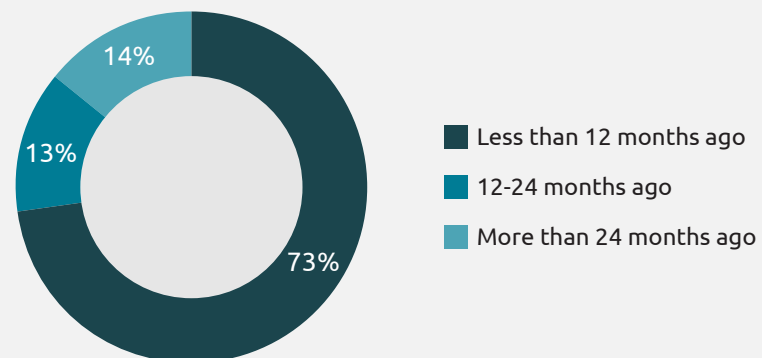## Smart factories: The new frontier in cyberspace

40% of organizations have been victim of a cyberattack that impacted their smart factories

Has your organization been a victim of a cyberattack that impacted your smart factories?

Industry	%
Heavy industry	51%
Pharma and life sciences	44%
Overall	40%
Chemicals (including petrochemicals)	39%
Semiconductors and hi-tech	39%
Consumer products	38%
Automotive	36%
Aerospace and defense	33%

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

When did the last cyberattack take place?

- 14% — Less than 12 months ago
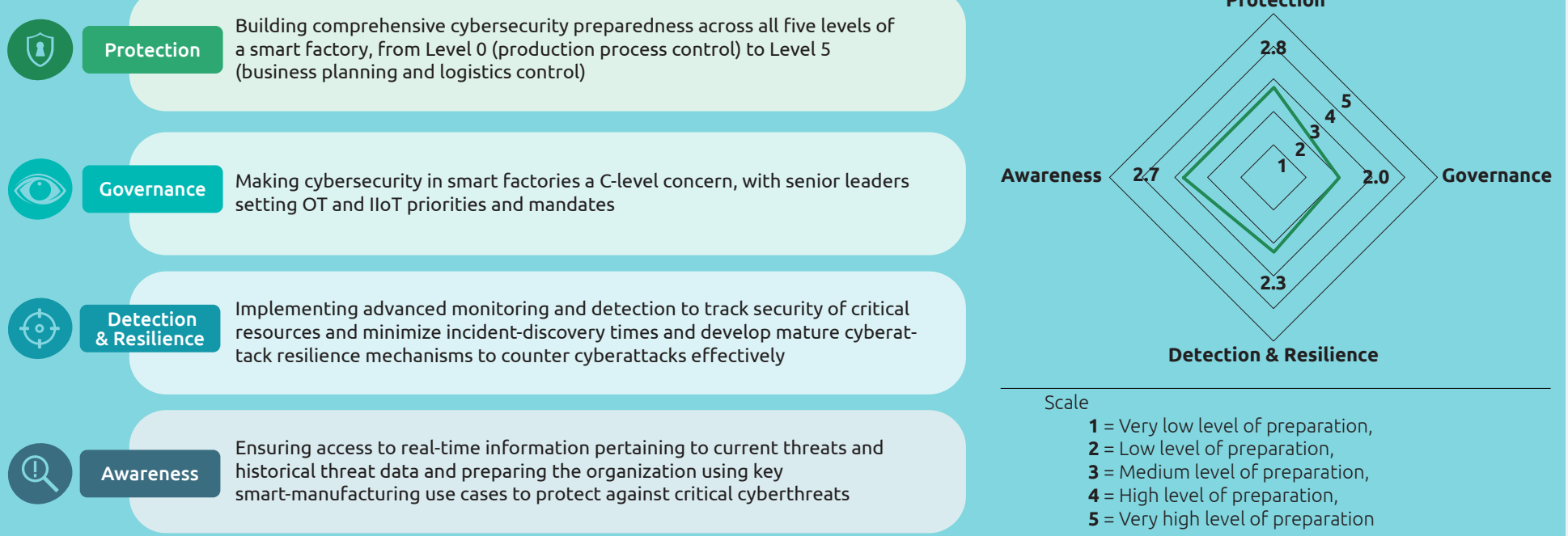- 13% — 12-24 months ago
- 73% — More than 24 months ago

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations

Organizations agree that cybersecurity is a critical component of smart factories

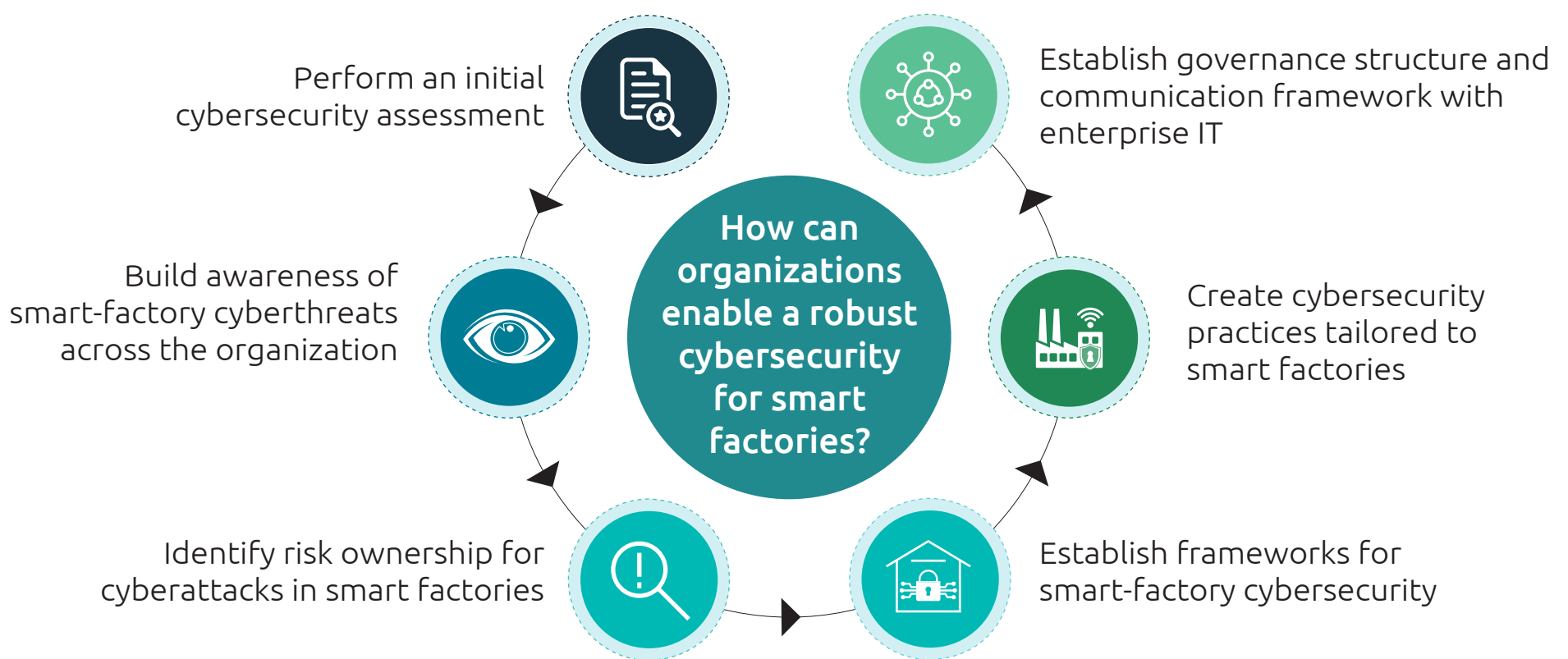**80%** Share of executives who view cybersecurity as a key component of a smart factory

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

Current levels of cybersecurity preparedness are low

Protection — Building comprehensive cybersecurity preparedness across all five levels of a smart factory, from Level 0 (production process control) to Level 5 (business planning and logistics control)

Governance — Making cybersecurity in smart factories a C-level concern, with senior leaders setting OT and IIoT priorities and mandates

Detection & Resilience — Implementing advanced monitoring and detection to track security of critical resources and minimize incident-discovery times and develop mature cyberattack resilience mechanisms to counter cyberattacks effectively

Awareness — Ensuring access to real-time information pertaining to current threats and historical threat data and preparing the organization using key smart-manufacturing use cases to protect against critical cyberthreats

Protection 2.8
Governance 2.0
Detection & Resilience 2.3
Awareness 2.7

Scale
1 = Very low level of preparation,
2 = Low level of preparation,
3 = Medium level of preparation,
4 = High level of preparation,
5 = Very high level of preparation

Source: Capgemini Research Institute, Cybersecurity in smart factories survey, October–November 2021; N=950 organizations.

How can organizations implement robust cybersecurity in smart factories?

How can organizations enable a robust cybersecurity for smart factories?

- Perform an initial cybersecurity assessment
- Establish governance structure and communication framework with enterprise IT
- Build awareness of smart-factory cyberthreats across the organization
- Create cybersecurity practices tailored to smart factories
- Identify risk ownership for cyberattacks in smart factories
- Establish frameworks for smart-factory cybersecurity

Source: Capgemini Research Institute Analysis

Download report

Subscribe to our research