

Keynote: Cybersecurity & Critical Infrastructure



Diarmuid Curtin
Cyber Partner
EY

OCA European OCPP Plug-fest and Conference

Cyber and critical infrastructure

September 2026



The better the question. The better the answer. The better the world works.



Shape the future
with confidence

Introductions



Diarmuid Curtin

Partner

UK&I Cyber Lead

State of the Cyber Landscape



1. **Geopolitical risk** looms large



2. **Opportunistic extortion** remains dominant risk



3. **Identity** is most often the *root cause of impact*



4. **Vulnerabilities & Third Parties** a growing challenge



5. **Social engineering** tactics outpace user awareness



6. **SaaS, APIs, & mobile** vectors



7. **Speed** is x-factor – **A.I. for offense** will tip scales

EV charging is becoming a connected critical service

EV charging is increasingly **relied-upon service** connecting transport, energy and digital infrastructure.

As that **reliance** develops, service **availability, integrity** and **recovery** become matters of **operational continuity** and **public trust**.

Criticality follows dependency

The significance of charging infrastructure is determined not only by the number of charge points, but by the extent to which **mobility and energy operations depend on coordinated charging services**.

Responsibility extends across the ecosystem

No individual organisation controls every component involved in delivering the service. **Resilience therefore depends on effective governance, common expectations and coordinated decision-making**.

Cyber risk requires leadership ownership

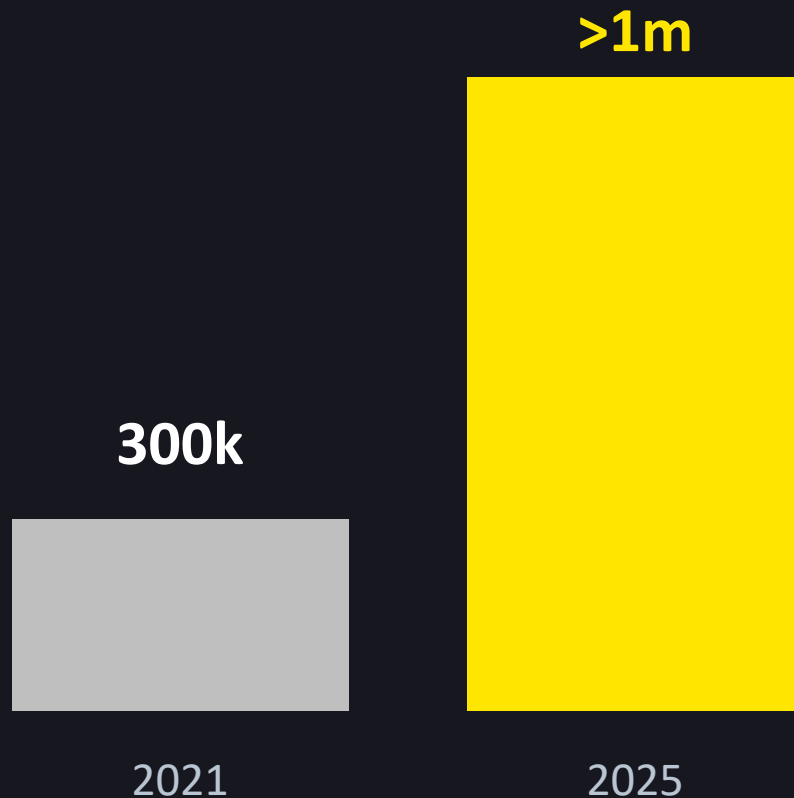
The relevant business issue is whether **essential charging services can remain safe, trusted and recoverable during disruption**.

EV charging becomes critical infrastructure when disruption can materially affect the services, systems and communities that increasingly depend upon it.

Moving from rollout to reliance

As adoption grows, availability and integrity become national resilience imperatives.

EU public recharging points



What has changed?

- 1 More endpoints** ➔ Increased number of physical and digital endpoints
- 2 Greater orchestration** ➔ Charging becomes actively managed, not passive
- 3 More dependency** ➔ Transport and energy operations rely on the same shared services
- 4 More consequence** ➔ A digital failure becomes a real-world disruption

Crossing trust boundaries

Energy, identity, payments, software and mobility converge in seconds.



Transaction dependencies



Vehicle & driver identity



Payment, roaming & mobile services



Charge point hardware & firmware



Grid signals & smart-charging logic



Communications & cloud platform



Maintenance and third-party access

When digital trust fails, the impact becomes physical

The risk is disruption at scale, not a compromised screen.



Disrupt : Charging unavailable

- Journeys delayed
- Fleets grounded
- Public confidence impacted

Manipulate : Altering of context

- Operational instability
- Billing disputes
- Grid concern

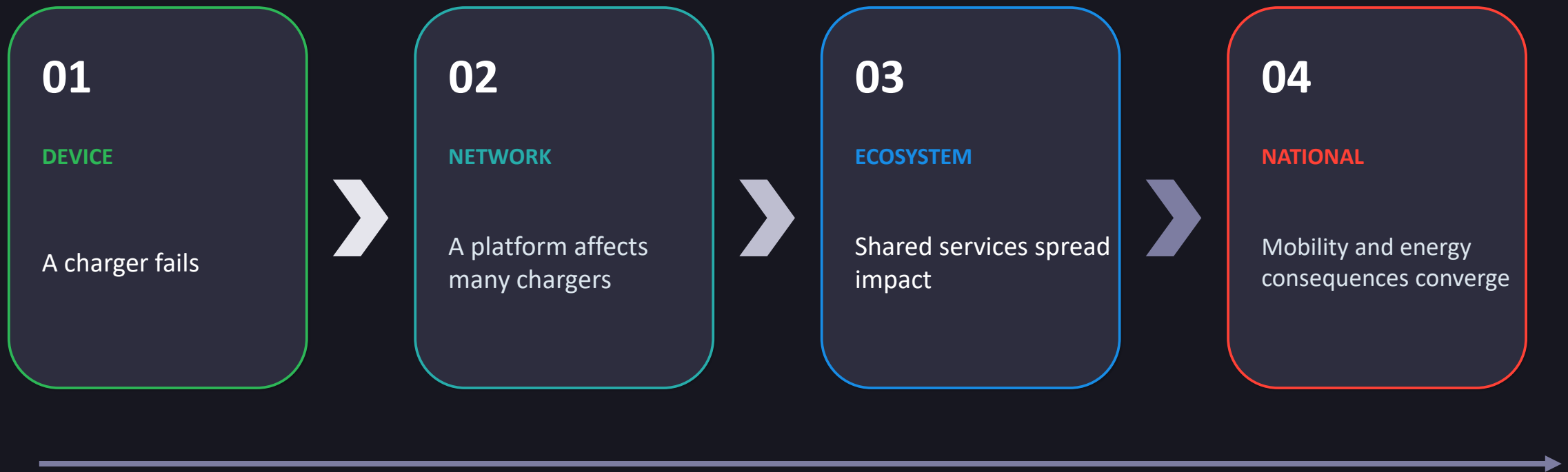
Exploit : A route into connected services

- Data exposure
- Supplier compromise
- Service and enterprise impact

Key question: what level of service must remain available during a cyber incident?

The risk changes as networks converge

Connectivity creates efficiency. Coordination can also create concentration.



Increasing dependency, coordination and potential blast radius

The biggest gap is often not the technology

Resilience is an outcome, but accountability is fragmented.



Four questions every ecosystem needs to answer

- 1 Ownership** ➤ Who owns the end-to-end service risk?
- 2 Visibility** ➤ Who can detect cross-party disruption?
- 3 Act** ➤ Who can isolate, communicate and recover?
- 4 Evidence** ➤ What evidence demonstrates resilience?

Key point : A contract boundary is not a resilience boundary.

Standards create capability. Operations create resilience.

Compliance is the floor. Trust is earned through sustained performance.

EU policy & regulation

AFIR interoperability and user experience • NIS2 risk and resilience expectations • product security obligations

Industry standards

OCPP security functions • IEC 62443-aligned component and system requirements

Assurance

Secure procurement • independent testing • certification • vulnerability evidence • supplier oversight

Secure operations

Identity • certificates • updates • logging • monitoring • incident response • recovery exercises

Key takeaway: Protocol support ≠ secure implementation ≠ resilient operation

Six Capabilities build trusted eMobility

The goal is safe, observable and recoverable service at ecosystem scale.



Secure by design, interoperable by default, availability as non-negotiable

Three moves to build trust before dependence deepens

Make cyber resilience part of the growth model.



5 questions that leaders need to ask

01

What level of EV-charging service must remain available during a cyber incident?

02

Do we understand and have we mapped the critical dependencies across chargers, platforms, identities, payments, energy systems and suppliers?

03

Is accountability clear across the ecosystem, including who can detect, declare, coordinate and lead recovery from an incident?

04

Have we assessed supplier, software and shared-platform dependencies that could create concentration risk or disruption at scale?

05

Are we adequately funding and testing a threat-led resilience programme covering secure design, monitoring, coordinated response and recovery?

Is the ecosystem is ready to carry the level of dependence we are placing upon it?

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organisation, please visit ey.com.

©2026 Ernst & Young. All Rights Reserved.

CI_26_387. Produced by Creative (Ireland). 06/2026. ED none.

The Irish firm Ernst & Young is a member practice of Ernst & Young Global Limited. It is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business in the Republic of Ireland.

Ernst & Young, Harcourt Centre, Harcourt Street, Dublin 2, Ireland.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com