RECHARGE UK

REPRESENTING THE UK EV INFRASTRUCTURE INDUSTRY

REA

WWW.R-E-A.NET

Scaled Up Secure EV Charging

EV Charging Cyber Security Report

By The REA's Cyber Security Working Group

CONTENTS

RECHARGE UK

REPRESENTING THE UK EV INFRASTRUCTURE INDUSTRY

WWW.R-E-A.NET

Executive Summary

The UK's transition to electric vehicles (EVs) is key to reaching net-zero goals, but the rapid growth of EV charging infrastructure also brings cyber security risks. As chargepoints connect to the national energy grid and an increase in state and organised crime gang funded hacking increases, the charging stations and various software systems are a target for cyberattacks.

1. Cyber Security Threats can disrupt charging services, steal customer data, damage vehicles and even impact local energy grids.

2. Common Weaknesses include:

- Unsecured internet connections including none or limited encryption of SIMS, WiFi or Ethernet communications
- Weak or default passwords
- Outdated firmware
- Lack of encryption or multi-authentication across the system.

3. Hypothetical example: A depot with poorly secured chargers could be hacked, causing fleet downtime for public services like buses or refuse collection - and exposing sensitive operational data.

What's Required?

1. Compliance with UK regulations (such as the Cyber Assessment Framework and ETSI EN 303 645) that will become mandatory from 2028.

2. Trade Associations should collaborate and communicate with their members and provide support to prepare for the new regulations and threats.

3. Organisations must:

- Secure all hardware and software systems
- Implement resilience and security best practices
- Train staff on cyber risks and safe practices
- Work with suppliers who meet national security standards

The Industry's Role

1. Government, EV supply chain, Local Authorities, Trade Associations, landowners, and fleet operators must collaborate to secure infrastructure.
2. NCSC has advised organisations across the UK, to adopt a "no trust" security mindset. This requires the EV eco-system to implementongoing threat monitoring, regular updates, and secure system design to protect users and the grid.

This report outlines the risks, legal obligations, and best practices to help all stakeholders navigate and respond to the growing cyber threat to EV infrastructure.

As technology advances, and the use of AI becomes the norm, government and industry are collaborating to introduce new legislation and best practices for the energy and charging infrastructure sector. The UK Government will be enforcing a strict security, supported by the REA. Therefore, organisations practicing and providing a service within the sector will be required to comply with these standards in order to obtain a licence to operate.

1. UK Cyber Security Landscape

According to the NCSC Annual Review 2024[1]. the UK faces an 'enduring and significant' threat to its critical infrastructure due to hostile states, cyber criminals, funded organised crime groups (OCG's), and the rapid adoption of emerging technologies like AI. As of the most recent reporting period, the UK's National Cyber Security Centre (NCSC) responded to over 600 significant cyber incidents in the 12 months leading up to August 2025. These incidents typically involve attacks targeting critical national infrastructure, government departments, and high-profile organisations via third-party suppliers or services. The latest transport industry high-profile organisations are TFL, Jaguar Land Rover, and Heathrow's boarding platform software, impacting airlines across Europe.

This figure reflects a continued rise in both the volume and complexity of cyber threats facing the UK, with ransomware and supply chain compromises remaining among the most prevalent attack types.

The NCSC is increasingly concerned that limited industry knowledge, collaboration, and public awareness are leaving EV charging and energy networks vulnerable to growing threats to the UK's critical infrastructure networks[2]. Whilst progress is being made, the rapid expansion of the EV market means that continuous vigilance and improvement in cyber security practices are essential to protect this critical infrastructure.

1. Best Practices: The NCSC recommends implementing best practices across commercial operations and the EV eco-system. These include strong authentication, encryption, regular software updates, Cyber Essentials Plus certification, deception tools and network segmentation to protect chargepoints from cyber threats[3].

2. Collaboration: They encourage collaboration between chargepoint operators, manufacturers (vehicle and chargepoint), and cyber security experts to develop and maintain secure systems. This includes sharing threat intelligence and working together to address vulnerabilities through industry associations and forums.

3. Public Awareness: The NCSC also highlights the importance of raising public awareness about the potential risks and encouraging users to follow security best practices, such as using secure home networks and keeping their charging equipment updated.

2. Charging Ecosystem Cyber Security Risks in EV

The EV charging infrastructure has a spider's web of interconnections. Data is exchanged between vehicles, back-office providers (EMSPs), driver apps, CPOs, grid operators, and energy suppliers. This complexity increases the attack surface and connections.

Identified vulnerabilities include unencrypted data channels, weak firmware, lack of network segmentation, fake QR codes and inadequate authentication. These expose systems to denial-of-service attacks, payment fraud, and potential grid destabilisation.

[1] https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024

[2] https://www.ncsc.gov.uk/pdfs/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure.pdf

[3] https://www.infosecurity-magazine.com/news/uk-cyberattacks-surge-ncsc/

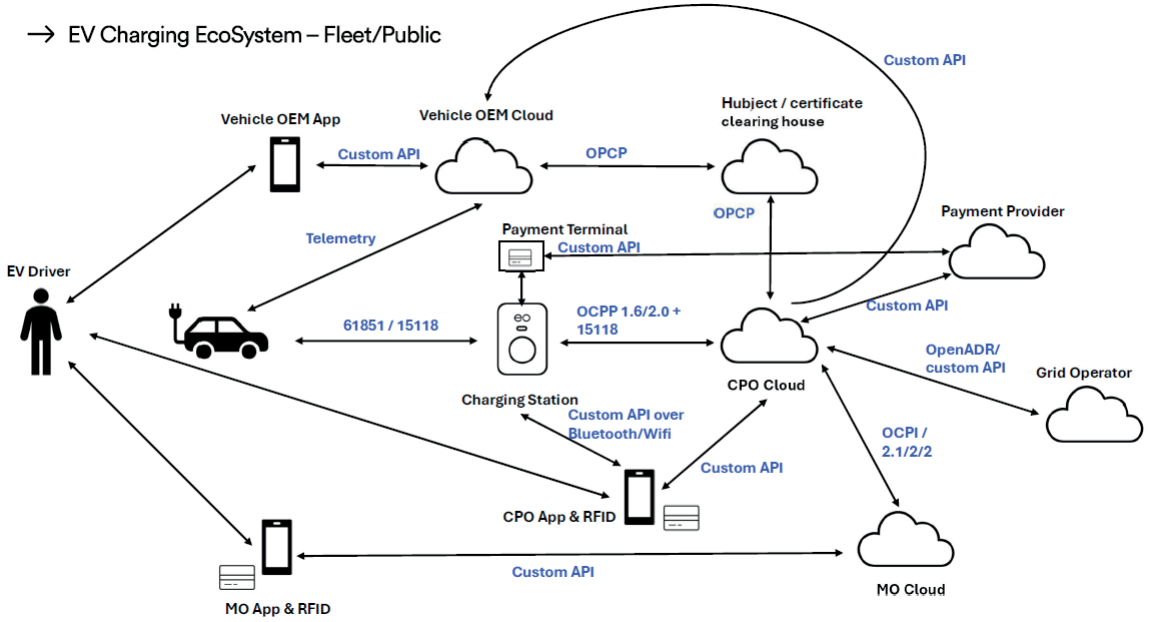

Fig 1: EV Charging Eco System Fleet/Public, Source: EO Charging

For domestic charging the ecosystem although complex is somewhat more streamlined.

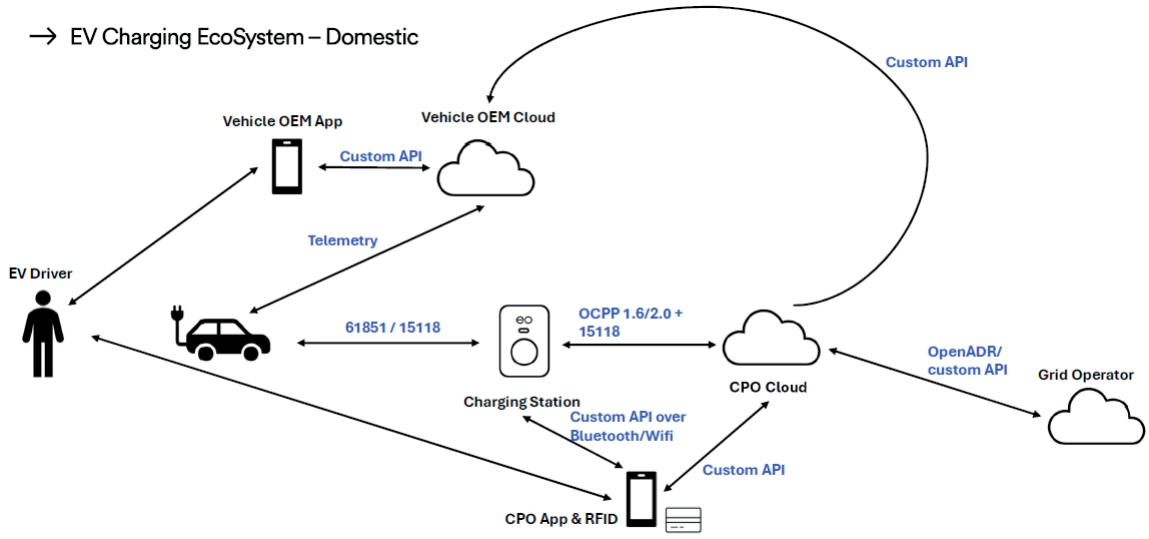

Fig 2: EV Charging Eco System Domestic, Source: EO Charging

All organisations that collaborate on the supply of products, software platform, service and maintenance or connections within this ecosystem have a responsibility for ensuring they are cyber resilient and secure.

3. Legislative and Regulatory Frameworks

The UK's legislators, regulators and industry representatives are supporting the evolving cybersecurity framework to address threats to critical infrastructure. The cornerstone legislation is the Network and Information Systems (NIS) Regulations 2018[4] designed to protect Operators of Essential Services (OES), including energy and transport sectors. These regulations are being updated through the forthcoming Cyber Security and Resilience Bill[5] to strengthen enforcement and expand coverage to include managed service providers and smart energy technologies provided by CPOs, Installers and EMSP's.

The EU's Cyber Resilience Act (CRA) and the Network and Information Security (NIS2) Directive, although not binding post-Brexit, it influences UK exporters and is shaping UK policy. The CRA mandates cybersecurity throughout the lifecycle of digital products, introducing common cyber security rules for manufacturers and developers of products with digital elements, covering both hardware and software. It has the potential to serve as a global benchmark beyond the EU's internal market. In addition, the NIS2 Directive establishes cyber security obligations - covering supply chain security and incident reporting - for essential and important entities, aiming to enhance the resilience of the services they deliver. The CRA and NI2 Directive also relate to the European Alternative Fuels Infrastructure Regulation (AFIR)6.

The European Commission recently adopted Delegated Acts to further specify the technical specifications outlined in Annex II of the regulation. This includes essential details on data standards, technical interfaces, and interoperability rules. The AFIR Delegated Act on Standards, which will apply from 8th January 2026, will require all newly installed or renovated publicly accessible charging points to support ISO 15118-2 from this date, and from 1st January 2027 all newly installed or renovated public and private charging points will be required to support ISO 15118-20.

The ISO 15118 standard is foundational to enabling Plug and Charge functionality - a seamless and secure method for authentication and authorisation services, without the need for RFID cards or apps. According to the AFIR Delegated Act on Standards all publicly accessible recharging points for AC and DC for light-duty and heavy-duty electric vehicles installed or renovated from 1st January 2027 that offer automatic authentication and authorisation services, such as Plug&Charge, should comply with both ISO 15118-2 and ISO 15118-20.

In addition, the Radio Equipment Directive for the EU (Aug 2025)[7] stipulates any device connected to the internet must now ensure network protection meaning radio equipment does not harm the network or its functioning nor misuse network resources. Radio equipment must also include safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected and ensures protection against fraud.

In the UK, the DESNZ led Smart and Secure Electricity System (SSES)[5] programme mandates that from 2028, chargepoint and load control operators meet cyber security requirements through standards such as ETSI EN 303 645[8] and profiles under the NCSC's Cyber Assessment Framework (CAF)[7].

The new Standards and Cyber Assessment Framework is significantly tighter including spot checks and license applications to access the market. CPOs and EMSP's will be required to comply with both the Host and Supply Chain cyber requirements. Taking

[4] https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[5] https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement/cyber-security-and-resilience-bill-policy-statement

[6] https://eur-lex.europa.eu/eli/reg_del/2025/656/oj

[7] https://www.bsigroup.com/siteassets/pdf/en/products-and-services/bsi_radio_equipment_directive-cybersecurity_faq_flyer_a4_241014.pdf

[8] https://www.gov.uk/government/publications/etsi-industry-standard-based-on-the-code-of-practice

the advancements of technology, including AI and quantum computing into consideration, the legislation is to be annually reviewed with higher penalties for non-compliance and loss of license.

4. Smart And Secure Electricty System (SSES)

The Department for Energy Security and Net Zero (DESNZ) through the Smart and Secure Electricity System (SSES) framework are setting minimum levels of cyber security for large load controllers of 300MW or more. Earlier this year it was also confirmed that DSR load controllers below 300MW will have a separate profile and will be for domestic and small nondomestic charging only. This will be achieved through the eventual inclusion to the Network and Information Systems (NIS) Regulations as Operators of Essential Services and following the corresponding Cyber Assessment Framework, with a tailored CAF profile to be consulted on this year (2025).

Timeline - what's happend so far and what's next?

During 2024, the SSES commenced consultations with industry and completed business and security architecture designs, enabling a business case to be written.

The following actions are:

2025
- Further technical consultations to develop the SSES framework.

2026
- Minimum Energy Smart Appliances (ESA)
- Standardised Interoperable Time of Use (ToU) - access to tariff data for flexibility services.
- DSR Service Provider License Framework (e.g. energy producing technologies)

2027
- Industry Lead in Period

2028
- Full device and organisational Cyber Security, Consumer Protection and Interoperability Standards in force.

This year, we expect further technical consultations to come out on developing the SSES framework.

The framework includes:

- Standardised and interoperable Time of Use Tariff formats in place to improve accessibility of tariff data for flexibility services by 2026.
- Cyber security, consumer protection and interoperability standards and requirements in place for Demand Side Response capable devices (i.e. devices able to control the consumption and production of energy) and service providers by 2028.
- The Government confirmed their intention to update the Network and Information System (NIS) Regulations once Parliamentary time allows and until then to implement legal requirements to manage the cyber security of Large Load Controllers initially through the load control licence.
- It was confirmed earlier in 2025 that there would be two CAF profiles, one for Large Load Controllers (>300MW) including public charging and one for DSR load controllers below 300MW which would be for domestic and small nondomestic charging only[9].
- The Government has set out principles for their cyber security assurance framework which includes enabling companies to transition between CAF profiles.
- The SSES framework is part of a wider workstream by Government to ensure improved cyber security across operators of essential services. The Cyber Security Resilience Bill 2025 will also require organisations like Managed Service Providers and data centres, as Operators of Essential Services, to adopt enhanced cybersecurity standards, report incidents, and comply with regulatory oversight.

What is the NCSC's Cyber Assessment Framework (CAF)?

The **Cyber Assessment Framework (CAF)**[10] is a comprehensive tool developed by the UK's National Cyber Security Centre (NCSC) to evaluate and enhance the cyber resilience of organisations, particularly those providing essential services such as energy, healthcare, and transportation. Introduced to support compliance with the Network and Information Systems (NIS) Regulations, the CAF offers a structured approach to assess how effectively an organisation manages cyber risks to its critical functions. It is designed to be adaptable across various sectors and can be utilised for self-assessment or by external auditors and regulators.

The framework is organised into four high-level objectives, each encompassing specific principles:

1. **Managing Security Risk:** Establishing governance structures and risk management processes to understand and control security risks.
2. **Protecting Against Cyber Attack:** Implementing measures such as access controls, data security, and staff training to prevent attacks.
3. **Detecting Cyber Security Events:** Monitoring systems to identify potential security incidents promptly.
4. **Minimising the Impact of Cyber Security Incidents:** Developing response and recovery plans to reduce the consequences of incidents.

[9] https://assets.publishing.service.gov.uk/media/6808a2630324470d6a394eb2/SSES-consultation-response.pdf

[10] https://www.ncsc.gov.uk/collection/cyber-assessment-framework

Each principle is associated with specific outcomes and **Indicators of Good Practice (IGPs),** which help organisations assess their current capabilities and identify areas for improvement.

For organisations supporting National Critical Infrastructure, the CAF serves as a vital resource to ensure robust cyber security practices are in place, aligning with national standards and enhancing overall resilience against cyber threats.

5. Mandatory Requirements and Industry Best Practice

The following standards and frameworks form the basis for cyber security compliance and resilience in UK EV Charging infrastructure:

Industry Standards

- **IEC 61851:** Defines basic requirements for electrical and communication between the vehicle and charging equipment[11].
- **ISO 15118:** Ensures secure, authenticated communication for Vehicle to Grid, and Plug and Charge capabilities[12].
- **ISO 27001:** Establishes an information security management system for any organisation and operational systems[13].
- **OCPP 1.6 plus Security:** Defines optional Transport Layer Security (TLS) for encrypted communications, basic HTTP authentication, and support for digital certificates to enhance secure connections.
- **OCPP 2.0.1:** Incorporates encrypted communication between chargepoints and management systems as standard. Approved as an IEC Standard in 2024, IEC 63584[14].
- **OCPP 2.1:** Released 2025[15].
- **ETSI EN 303 645:** Cyber security standard for IoT devices, including EV chargepoints. This is now mandatory for Radio Equipment Directive compliance.
- **Cyber Essentials Plus Certification:** Organisations are required to hold this standard for operational and supply chain security where sharing, use or storage of 3rd party data.
- **NCSC Cyber Assessment Framework (CAF):** Defines expectations for risk management, system integrity, and supply chain security. The CAF is recommended for both large and small operators, with profiles tailored to load controllers above and below 300MW

As a minimum best practice requirements for regular firmware updates like signed firmware images with rollback protection to prevent tampering or malicious updates, secure APIs, TLS encryption (TLS 1.3 >), and PKI certificate management. Cyber training for all individuals across the business operation and engagement are required to ensure there is clarity on the potential risks to the businesses and processes and practices individuals need to follow such as multi-authentication and use of a VPN between the charging station and back-office system.

Cyber Essentials Plus also requires regular cyber penetration testing; this is where an approved 3rd party is permitted to carry out a "Friendly Cyber Attack" with agreed regularity. The organisation will not be notified of the planned attack and upon completion will receive a report to advise them of their security weaknesses and actions to be taken to prevent a "non-friendly" attack.

NCSC, Dept. of Transport, and Dept. for Energy Security and Net Zero Guidance

The NCSC promotes the adoption of the Cyber Essentials scheme, and through its annual review, highlights the increasing cyber threat to Critical National Infrastructure (CNI). It provides incident response capabilities and encourages adoption of secure-by-design principles. DESNZ reinforces this by mandating CAF usage for load controllers and aligning smart appliance cyber security with existing EV chargepoint requirements.

[11] https://ses.jrc.ec.europa.eu/eirie/en/standard-regulations/electric-vehicle-conductive-charging-system-part-1-general-requirements-0

[12] https://wevo.energy/glossary/what-is-iso15118/

[13] https://www.iso.org/standard/27001#:~:text=ISO/IEC%2027001%20is%C2%A0the%20world's%20best-known%20standard

[14] https://openchargealliance.org/protocols/open-charge-point-protocol/

[15] https://openchargealliance.org/protocols/open-charge-point-protocol/
ISO15118 eco-system - https://www.hubject.com/ecosystem-overview

What is ISO 15118?

While ISO 15118 compliance will become mandatory under AFIR in Europe, it should also be recognised as a strategic enabler of security whose adoption in the UK would further support security improvements.

Key benefits include:

- End-to-end encryption of communications between the EV and the charging station.
- Mutual authentication using PKI certificates, preventing rogue devices from connecting to the grid.
- Secure support for Plug & Charge, protecting credentials and reducing risks of spoofing or cloning.
- Mitigation of man-in-the-middle and replay attacks through strong cryptographic protections.

What is ETSI EN 303 645?

ETSI EN 303 645 is a European cyber security standard developed by the European Telecommunications Standards Institute (ETSI) to establish a baseline of security for consumer Internet of Things (IoT) devices. First published in 2020, the standard focuses on protecting network-connected products, including Chargepoints, from widespread and easily exploitable cyber threats.

Key provisions are:

- Removal of universal default passwords
- Secure storage of sensitive data
- Regular software updates
- Encrypted communications
- Ease of personal data deletion
- Embedding fundamental security principles into product design and operation.

The standard is outcome-focused and supports regulatory alignment with frameworks such as the UK's Product Security and Telecommunications Infrastructure (PSTI) Act and the EU Cyber Security Act. To assess conformance, ETSI provides a companion specification that guides manufacturers and testing bodies through evaluation methods. Compliance can be self-declared or independently verified, and it serves both as a benchmark for best practice and a stepping stone toward future regulatory requirements.

6. Operational Best Practice

In addition to GDPR requirements, the following are considered a minimum list of requirements when procuring or permitting the installation of charging infrastructure. For confirmation of compliance, we recommend organisations source proof of compliance from installers, CPOs and EMSP's.

1. **ChargePoint Operators:** Ensuring the switching on of security protocols within OCPP, OCPP 2.01 or later, Cyber Essentials Plus, alignment with ISO 27001and ISO 15118.
2. **Communication providers:** 4G/5G, fibre, data satellite. All require a resilient, secure and stable service, regardless of communication type and interface between charging stations and back-office platforms. This helps to minimise outage from cyber-attack, atmospherics, and cell mast failure, etc). recommended for both large and small operators, with profiles tailored to load controllers above and below 300MW.
3. **IT System Integrators:** Enterprise grade integration of complex IT backend systems and an ecosystem of 3rd parties that share their cyber security practises, and joined through secure, encrypted connectivity.
5. **OT System Providers:** Must ensure a stable, end-to-end management of Operational Technology (OT) hardware assets involved in charging infrastructure, including Transformers and robust communication. Through consolidation of communications, it is advisable to use Edge security and a firewall to protect on-site hardware from cyber-attack, and use of diversion tools to limit impact of on-site attacks on back-office systems.
6. **Smart Energy Load Balancing:** Regular review of load balancing software and in line with energy providers testing schedules to check for weaknesses and compliant with current and future requirements under the Cyber Security Framework.
7. **SIM:** Chargepoints have encrypted SIMS installed. SIMS connecting via a private APN are significantly harder to hack, due to their "invisibility" to the internet and hackers.
8. **Offline Mode:** Ability for charging sites to continue to operate when communication to back-office systems fail, or back-office systems go offline. Mechanism to cache transactions (eg card payment, RFID, EV certificate) until such time that "online mode" is restored. This protects CPO brand reputation and reduces risk of lost revenue.

Separately to this report we understand OZEV are seeking to work with industry to improve cyber resilience across the public charging space.

7. Standard Requirements for Tenders

It is essential to incorporate cyber resilience and security within tender technical specifications. Not all organisations are compliant with the latest legislation and requesting proof of certification and practises is key to ensure peace of mind when procuring charging infrastructure.

The table below provides guidance on what to include within technical specifications as standard.

Aspect	Public Charging	Private Charging	Depot Charging
Cyber Security Requirements	Implement **Open Charge Point Protocol (OCPP)** 1.6 plus security as a minimum or 2.0.1 for secure communication between charging points and management systems. Comply with **ISO 15118** for secure vehicle-to-grid (V2G) and plug-and-charge capabilities to adopt maximum security profiles available. Adhere to **NIS2 Directive** for critical infrastructure cyber security measures.	Ensure secure Wi-Fi configurations with **WPA3** encryption, including advising home consumers to adopt WPA3 encryption on their home WiFi. Use strong, **unique passwords** for device access. Regularly **update firmware** to patch vulnerabilities.	Implement **ISO 27001** for comprehensive information security management. Utilize **VPNs and firewalls** for network security. **Employ endpoint detection and response (EDR)** systems for continuous monitoring.
Best Practices Using Existing Standards and Protocols	Utilise **TLS encryption** for secure data transmission. Implement **PKI-based certificates** for mutual authentication. Ensure secure **firmware updates** to maintain system integrity.	Configure **WPA3** for robust Wi-Fi security. Set **strong, unique passwords** for all devices. Perform **regular firmware updates** to address known vulnerabilities.	Adopt a **zero-trust architecture** to verify all network access. Implement **multi-factor authentication (MFA)** for system access. Conduct **continuous monitoring and regular penetration testing** to identify and mitigate threats.

Communications & Connectivity Requirements

Chargepoint communications must be:

- Reliable and resilient to maintain continuous operation.
- Ethernet (RJ45), Wi-Fi with WPA3 encryption and strong passwords.
- Mobile networks accessed through encrypted roaming SIM cards.

Communication hardware must:

- Both integrated and external communications hardware (modems/ routers/mobile phone boosters) must be encrypted preferably with a dynamic connection to the back office and or network onsite.
- Security & Data Protection.

Chargepoints must:

- Use TLS encryption and PKI based certificates for mutual authentication to ensure secure firmware updates.
- Support the Open Charge Point Protocol (OCPP) 2.0.1 minimum.
- Remain compatible with third-party systems in the future.
- Anti-tamper switches on the hardware.
- Servicing and maintenance programmes shared with all stakeholders for clarity on expected hardware access.
- Anti-tamper on metering and switch panels.
- QR codes are protected from fraudulent stickers for fake registration websites.
- Rollback software updates to avoid stranded assets.

CPOs must:

- Be certified to ISO 27001 (international information security standard).
- Use VPN's, Firewalls for network security.
- Deploy endpoint detection and response (EDR) systems.
- Have a Security Plan with trained personnel to manage risks.
- Protect all data transfers, including via USB/removable media.
- Enforce strict access control to prevent unauthorised changes.
- Implement multi-factor authentication (MFA) for accessing back-office platforms.
- Quarterly penetration testing as a minimum to identify and mitigate threats.

Communication and payment systems must provide proof of compliance before contract delivery:

- Payment Card Industry Data Security Standards (PCI DSS).
- Cyber Essentials Plus Certification
- Compliant with ETSI EN 303 645 (IoT cybersecurity standard).

Operational cyber security

- Regularly apply software and firmware updates to fix vulnerabilities.
    - Plans should be shared with commercial clients of when updates are to be made and testing to ensure the chargepoints do not go offline.

- Follow a planned upgrade roadmap agreed with the commissioning body.
- Maintain ongoing cyber security updates and protections.
    - Updates can be shared but details of security patches should not be shared, to ensure weaknesses in previous versions are not published and exploited by hackers while live on other devices.
- Use only products that have been security tested and accredited.

8. Further Recommendations

1. Establishment of a UK specific EV Charging ISAC

A dedicated EV Charging Information Sharing and Analysis Centre should be created to co-ordinate threat intelligence across the sector.

The ISAC would serve as a trusted platform where CPOs, eMSPs, manufacturers, grid operators, and government can share real-time threat data, incident response strategies, and lessons learned. With a rising number of cyber security attacks across the UK, this could be a way for industry to share, adapt and learn from one another to protect customers.

With REA member GreenFlux having a leading role in this area, as one of the co-founders of the first EV-specific ISAC in the Netherlands, (EVC ISAC) is a useful case study to support the UK to utilise a proven ISAC model. This could help reduce incident response times, prevent duplication of effort, and improve situational awareness across the EV charging ecosystem.

2. Application of IEC 62443 Principles

EVSE systems share many characteristics with industrial control systems and OT. Applying IEC 62443 standards can significantly increase resilience:

- Defence-in-Depth Architecture: Isolate IT and OT systems and restrict lateral movement with network segmentation.
- Zones and Conduits: Group assets (backend, chargepoints, grid connections) into defined security zones with controlled communication pathways.
- Secure Development and Components: Suppliers should adhere to IEC 62443-4-1 (secure product development lifecycle) and IEC 62443-4-2 (technical security requirements for components).
- Patch and Vulnerability Management: Ensure structured handling of vulnerabilities with timely patch deployment and lifecycle support for long-lived EVSE hardware.
- Role-Based Access Control: Enforce identity and access management across all EVSE assets, with strict logging of physical and remote access.


CO2
WARNING

9. Skills Landscape

The rapid evolution of the electric vehicle (EV) sector - particularly in charging infrastructure and digital connectivity - has introduced new skills requirements across both public and private sector stakeholders. A secure, resilient EV ecosystem demands:

- **Cyber-aware engineers and technicians** involved in chargepoint installation and maintenance
- **Procurement and contract managers** trained to assess cyber resilience in supply chains and vendor solutions
- **IT and network specialists** skilled in EV software platforms, protocols (e.g. OCPP), firmware updates, and threat monitoring
- **Local Authority officers** with baseline cyber literacy to assess risk and respond to incidents

There is a pressing need to **upskill the workforce,** embed cyber security awareness into existing training programmes, and ensure consistent standards across energy infrastructure providers, chargepoint operators (CPOs), installers, and fleet managers.

Opportunities

The intersection of transport, energy, and digital infrastructure presents significant opportunities:

- **Green Tech Careers:** Cyber security within the EV ecosystem offers rewarding roles in a future-proof sector that aligns with sustainability goals.
- **UK Leadership in Secure Smart Infrastructure:** By embedding cyber security from design to deployment, **the UK can lead in setting global standards for secure EV infrastructure.**
- **Innovation in Secure-by-Design Solutions:** Hardware and software providers can develop and commercialise chargepoints with embedded cyber protection (e.g. encrypted communications, automated patching, and endpoint protection).
- **Stronger Public-Private Partnerships:** Collaboration between Local Authorities, chargepoint operators, and central bodies like the NCSC fosters a coordinated defence against cyber threats.

Key Concerns

Despite the opportunities, there are growing concerns that threaten both operational resilience and public confidence:

- **Lack of standardised cyber training** for chargepoint installers and EV service providers
- **Limited cyber awareness at Local Authority level,** especially when managing public tenders and deployments
- **Fragmented supply chains** increase vulnerability to compromised firmware, unpatched systems, and third-party risk
- **Cyber threats targeting EV infrastructure as a gateway to wider Critical National Infrastructure (CNI),** including smart grids, transport networks, and emergency services
- **Data privacy risks** from vehicle-user interactions, payment systems, and mobile app integrations

Failure to address these concerns could result in data breaches, operational downtime, or systemic infrastructure attacks - reinforcing the need for robust governance, workforce training, and shared responsibility across all levels of the EV value chain.

10. REA Cyber Security Working Group Members

Thanks to the REA Member Cyber Security Working Group for helping inform and produce this report. In particular to Katie Colledge Price, Tony Shorthouse and Richard Earl for their important contributions and time spent helping galvanise support from industry for this report.

BEAT
Better Environment And Transport

WWW.BEATZERO.CO.UK

CSL

WWW.CSL-GROUP.COM

eo

WWW.EOCHARGING.COM

greenflux

WWW.GREENFLUX.COM

HUBJECT

WWW.HUBJECT.COM

JIGSAW POWER

WWW.JIGSAWPOWER.COM

MOBIUS
NETWORKS

WWW.MOBIUSNETWORKS.CO.UK

PluginPOWER

WWW.PLUGIN-POWER.COM

Find out more and support the sector

For further information, please contact:

Matt Adams
Head of Transport, REA
madams@r-e-a.net

Aisha Afeef
Communications Executive, REA
aafeef@r-e-a.net

If you're interested in REA membership, please contact:

Lindsay Barnett
Director Membership, Marketing & Events, REA
lbarnett@r-e-a.net

The report is available on the REA website, here:

https://www.r-e-a.net/our-resources/

Follow us on X or LinkedIn:

@REAssociation|renewable-energy-association
www.r-e-a.net

RECHARGE UK
REA, York House, 23 Kingsway
London WC2B 6UJ

WWW.R-E-A.NET

RECHARGE UK

REPRESENTING THE UK EV INFRASTRUCTURE INDUSTRY

REA

WWW.R-E-A.NET