Driving Digital Trust and Sustainability

How ISO 27001 protects the data that underpins ESG and why it matters now

The Global Cyber Threat Landscape

Cyber attacks are no longer exceptional events. They are the permanent operating environment for every organization on the planet. The question is no longer whether an organization will face a cyber incident, but when and whether it will be prepared.

The data for 2024 - 2025 tells a stark story of accelerating frequency, escalating cost, and rapidly evolving tactics. In Q1 2025, the average organization faced 1,925 cyber attacks per week, a 47% rise from the same period in 2024 (*Check Point Research*). Global cybercrime costs are projected to exceed $10.5 trillion annually by 2025, representing a 10% year-on-year increase (*CompTIA*). The average cost of a single data breach reached $4.88 million in 2024 (*IBM Security*) and in sectors like healthcare, that figure climbs to $9.77 million per incident.

The attack methods organizations face today

The threat landscape has diversified significantly. No single attack type dominates - instead, threat actors combine tactics, using automation and AI to increase both volume and precision:

Ransomware:

Attacks rose 126% in Q1 2025 versus Q1 2024 (*Check Point Research*), with 2,289 publicly reported incidents in a single quarter. Manufacturing, consumer goods, and business services are the hardest hit. The 'double extortion' model, encrypt data AND threaten to publish it, has become standard practice, with 62% of manufacturing ransomware victims paying the ransom demanded (*Viking Cloud, 2024*).

Phishing and social engineering:

Still the most common initial access vector. 82.6% of phishing emails now use AI technology in some form, and 78% of recipients open AI-generated phishing emails (*Tech Advisors, 2025*). Voice phishing (vishing) surged 442% between the first and second halves of 2024 (*CrowdStrike*). In 2024, 79% of successful attacks used no malware at all, instead exploiting stolen credentials, trusted tools, and human behaviour.

Supply chain attacks:

75% of software supply chains experienced a cyberattack in the last 12 months (*BlackBerry, 2024*). These attacks are particularly dangerous because they are hard to detect and have the highest potential blast radius, a single compromised vendor can expose hundreds of downstream organizations simultaneously.

Nation-state and geopolitical attacks:

Chinese cyber espionage operations surged 150% overall in 2024, with attacks on financial, media, and manufacturing sectors rising to 300% (*CSIS, February 2025*).

Deepfakes and synthetic identity fraud:

47% of organizations have already experienced a deepfake attack (*iProov*). AI-generated voice clones and video deepfakes are now used to impersonate executives and authorise fraudulent transactions. In a high-profile 2024 case, a finance employee was deceived by a deepfake video call into transferring $25 million to fraudsters.

AI as a threat amplifier and a hidden internal risk

Artificial intelligence is transforming the cyber threat landscape from two directions simultaneously: as a tool in the hands of attackers, and as an unmanaged data risk within organizations themselves.

On the attacker side, AI enables threat actors to craft more convincing phishing messages, scale attacks at unprecedented speed, generate realistic deepfakes, and discover vulnerabilities faster than human security teams can respond. Generative AI tools allow attackers to compose phishing emails up to 40% faster, and the sophistication of AI-generated content means traditional detection methods are failing. Gartner predicts that 17% of all cyberattacks will employ generative AI by 2027.

Inside organizations, however, a less visible, but equally serious, risk is rapidly growing: employees using public AI tools to handle sensitive business data without organizational oversight. This phenomenon, known as 'Shadow AI', represents a fundamental shift in how data leaves an organization's control.

38%

of employees share sensitive work data with AI tools without employer permission

CybSafe/NCA Global Survey, 2024 (7,000 respondents)

47%

of generative AI platform usage in enterprises occurs via personal accounts with no company oversight

Netskope, 2025 (based on Oct 2024–Oct 2025 cloud analytics)

223

data policy violations involving GenAI applications per organization, per month - on average

Kiteworks/AI Data Security Report, 2026

What types of data are employees sharing?

Source code accounts for 42% of AI-related data policy violations - developers are the heaviest AI users in most organizations, routinely uploading proprietary code for debugging help (*Kiteworks, 2026*). The rest includes client data, financial records, contracts, strategic plans, and ESG-related information such as sustainability targets, supply chain data, and human rights assessments. OpenAI's own user guide states: 'We are not able to delete specific prompts from your history. Please don't share any sensitive information in your conversations.'

The consequences are already materialising

1 in 5 UK companies has experienced a data leakage incident caused by employees using generative AI (*UK CISO survey, 2024*). Samsung banned internal AI tool use entirely in 2023 after employees shared source code and meeting notes with ChatGPT. Gartner warns that 40% of organizations will experience a Shadow AI security incident by 2030 - and 69% of cybersecurity leaders already have evidence or strong suspicion that employees are using public AI tools at work today.

For organizations with ESG reporting obligations

the risk is particularly acute. Employees working on sustainability disclosures, GHG data, supply chain audits, and human rights due diligence routinely handle precisely the kind of sensitive, material, and regulated information that should never be shared with an unsecured third-party AI platform. Without the governance controls ISO 27001 provides, data classification, access management, acceptable use policies, and awareness training, organizations are creating an invisible data leakage channel they may not even know exists.

The new frontier of cyber risk is not always external. It sits inside every organization, in the browser tab where an employee pastes a sustainability report draft into ChatGPT, or uploads a supplier audit to an unmanaged AI tool. Shadow AI is the data breach that hasn't happened yet. ISO 27001 provides the governance framework to close it before it does.

The Global Impact of Data Breaches

$4.88M
average cost of a data breach
IBM Security, 2024

1925
global weekly attacks per org
Check Point Research, Q1 2025

47%
increase in attacks Q1 2025 VS Q1 2024
Check Point Research, Q1 2025

Most targeted sectors globally (weekly attacks per organization):

Education & Research
4175
#1 globally for 4th consecutive year; +3% YoY
Check Point, Q1 2025

Telecommunications
2703
+6% YoY; high-value data & critical services
Check Point, 2025

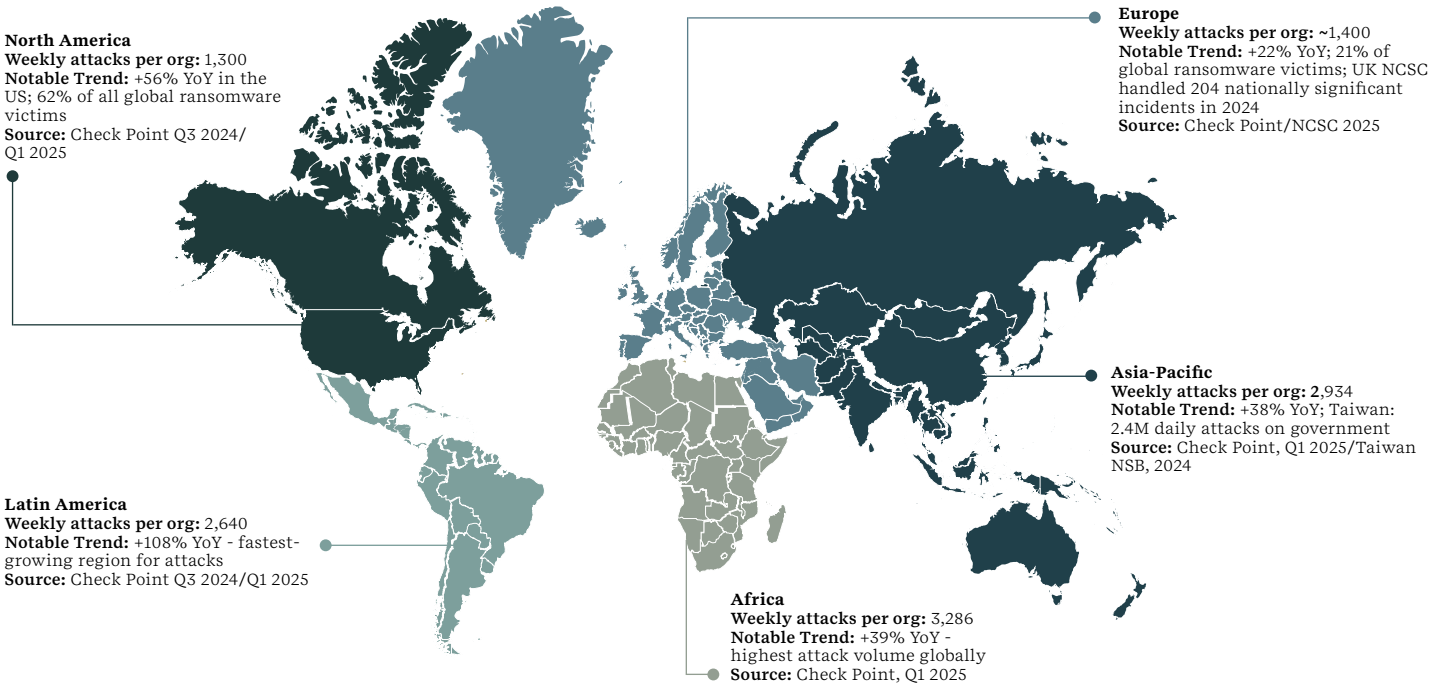
Government/Military
2512
–6% YoY but still critically targeted; state espionage driver
Check Point, 2025

Healthcare
2434
+110% YoY (Q3 2024); avg breach cost $9.77M
Check Point Q3 2024; IBM 2024

Manufacturing
~1800+
#1 for ransomware (30% of all victims); 4th consecutive year as most-breached sector; avg breach cost $5.56M
Check Point Q3 2024; IBM X-Force 2024

Finance & Insurance
~1600+
65% hit by ransomware in 2024; malicious bot requests +69% YoY; avg breach $5.9M
Statista 2024; Viking Cloud 2024

Regional picture (weekly attacks per organization):



The Impact on ESG Targeted Data

Sustainability data has become financially and reputationally critical. Investors, regulators, and customers base capital allocation and procurement decisions on the quality and integrity of ESG disclosures. This makes ESG data an increasingly high-value target, and a single breach can destroy the trust that takes years to build.

ESG Data Type	Why Attackers Target It	Potential Impact of a Breach
GHG inventories & emissions data	Manipulation can mask non-compliance; theft exposes competitive decarbonization strategies	Regulatory fines (CSRD, SEC); investor withdrawal; reputational damage
Supply chain traceability records	Reveals supplier relationships, leverage points and commercial terms	Exposure of sourcing vulnerabilities; litigation under CSDDD / UK Modern Slavery Act
Human rights due diligence data	Contains sensitive worker, community and whistleblower information	Legal liability; NGO/media exposure; loss of operating licence
ESG ratings & disclosure data	Altering figures can affect capital access, index inclusion and ESG ratings	Fraudulent disclosures; regulatory investigation; investor litigation
Board & governance records	Insider intelligence on risk positions and compliance gaps	Corporate espionage: governance failures exposed publicly

A breach damages more than IT systems, it damages credibility. The basis of ESG reporting is trust, and rebuilding it after a breach is slow and expensive. Regulators increasingly treat ESG data manipulation as a material governance failure.

The consequences of a breach affecting ESG data extend far beyond IT recovery costs. They cascade across financial, regulatory, reputational, and operational dimensions simultaneously.

Financial

- Average breach cost: $4.88M globally (IBM, 2024)
- Healthcare: avg $5.3M per incident (PwC, 2024)
- Extreme losses quadrupled since 2017 to $2.5Bn (IMF, 2024)
- Financial sector: $12Bn losses over 20 years (IMF, 2024)

Regulatory

- GDPR/UK GDPR fines up to 4% global turnover
- NIS2: up to €10M or 2% of global turnover
- SEC cyber disclosure requirements triggered
- CSRD: inaccurate ESG data is a disclosure risk

Reputational

- Loss of investor confidence and ESG rating downgrades
- Damaged digital trust with customers and partners
- Media exposure; NGO and activist scrutiny
- Brand value erosion - often irreversible

Operational

- Business shutdowns averaging 197 days to detect breaches
- Disruption to sustainability and decarbonization programmes
- Loss of ESG audit evidence and reporting continuity
- Supply chain disruption and third-party contractual breaches

The benefits of ISO 27001 for ESG data, connecting cyber trust with ESG integrity

ISO 27001 is primarily an Information Security Management System (ISMS) standard, but its principles and controls directly support sustainability and ESG objectives across all three pillars. The table below maps specific ESG requirements to the ISO 27001 controls that underpin them. ISO 27001 does not operate in isolation. It sits alongside and supports a family of regulations and frameworks that together define what good governance of information and ESG data looks like.

Environmental	Social	Governance
Efficent, Low-Waste Digital Operations - Enables secure digitization, reduces paper dependency, and elimates physical storage waste.	**Data Privacy & Human Rights** - Protecting personal and stakeholder data reinforces social responsibility and ethical digital practices.	**Accountability & Regulatory Compliance** - Strengthens governance through leadership oversight, risk-based control frameworks, and compliance with global regulations. Mandatory leadership responsibilty.
Energy-Optimized IT Infrastructure - Encourages modernized, energy efficient data centres and cloud platforms with lower carbon footprints, contributing to carbon reduction goals.	**Cubersecurity Awareness & Training** - ISO 27001 mandates employee training, fostering a culture of accountability and shared responsibility.	**Integrity of ESG Data & Reporting** - Protects the accuracy and reliability of climate, sustainability, and financial-ESG disclosures, ensuring credible, traceable and assurance ready ESG disclosures. ISO 27001 is a key internal control.
Sustainable Tehnology Lifecycle - Strengthens responsible procurement, reuse, and recycling of IT assets to minimize e-waste.	**Transparency & Stakeholder Trust** - Demonstrates ethical handling of information, strengthening confidence among employees, customers, and communities.	**Robust Risk & Supply-Chain Governance** - Enhances enterprise risk management and ensures responsible oversight of third-party partners.

Why ISO 27001 matters for sustainability professionals

Cybersecurity is not just an IT issue; it's a strategic enabler of sustainability and ESG goals

Cybersecurity is now a core ESG enabler - protecting the integrity of climate, sustainability, and financial-ESG data, ensuring disclosures remain credible and assurance-ready.

Safeguards sustainability infrastructure including smart grids, renewable energy systems, and IoT supply chains, preventing cyber incidents that disrupt decarbonization and critical services.

Reduces environmental impact of digital operations through secure cloud adoption, efficient data centers, lifecycle management, and disruption of energy-wasting cybercrime (e.g., botnets, crypto-mining malware).

Strengthens governance and stakeholder trust by embedding risk-based controls, regulatory compliance, and ethical data handling across the organization.

Protects social responsibility commitments by securing personal and stakeholder data, reinforcing transparency, accountability, and community trust.

Supports operational resilience - ensuring business continuity, reducing the resource impact of cyber incidents, and maintaining progress toward sustainability and ESG targets

Why ESG and sustainability matters for cyber/infosec professionals

Sustainability and cybersecurity are deeply interconnected, shaping strategy, compliance, and enterprise risk management

ESG regulations now include cyber requirements

meaning security teams must protect sustainability, climate, and ESG data to maintain compliance and avoid reputational or legal risk.

Cybersecurity protects critical sustainability infrastructure

including smart grids, renewable energy systems, and IoT supply chains , preventing attacks that could derail decarbonization and operational resilience.

Green cybersecurity reduces environmental impacts

from cutting energy-intensive data center operations to minimizing e-waste and stopping botnets and crypto-mining attacks that waste massive amounts of electricity.

Investors and stakeholders view cyber resilience as a material ESG factor

making strong security essential to governance maturity, ESG ratings, and access to sustainable finance.

Cyber incidents directly disrupt sustainability progress

creating energy-heavy recovery processes, operational downtime, and loss of trust in ESG reporting and leadership commitments.

Aligning ISO 27001 with ESG goals strengthens integrated governance

enabling secure ESG reporting, energy-efficient IT practices, responsible procurement, and consistent sustainability performance across the organization.

Fundamental Principles for Success

Knowing the risks is only the first step. The organizations that protect their ESG data and governance reputation are those that treat information security as a cultural and strategic priority, not a technical checkbox. Three pillars underpin sustainable action:

Empowering People

Up to 95% of breaches are linked to human error (*Verizon, 2025*). Culture and awareness are your first line of defence.

- Leadership sets the tone - visible board sponsorship of security and ESG integrity is non-negotiable
- Role-based security training embedded across IT, sustainability, legal, and finance teams
- Phishing simulation and social engineering awareness - especially important given AI-generated attacks now account for 80%+ of phishing emails
- Clear escalation paths for reporting security concerns without fear
- Cross-functional collaboration: break silos between IT, sustainability, and compliance

Building Digital Literacy

Many ESG processes still rely on spreadsheets, email, and manual consolidation, making them high-risk by design.

- Understand what ESG data exists, where it lives, and who has access to it
- Apply ISO 27001 Competence and Awareness requirements (Clause 7.2 / 7.3) to sustainability roles
- Train ESG and sustainability teams on data classification, handling, and incident recognition
- Embed data integrity checks and version control into sustainability reporting workflows
- Establish clear ownership of ESG data assets, not just IT systems

Security, Integrity & Continual Improvement

ISO 27001's Plan-Do-Check-Act cycle ensures security and ESG governance improve continuously, not just at audit time.

- Formal risk assessments that include ESG data as a critical asset category
- Audit trails, logging, and evidence retention for all sustainability reporting systems
- Regular internal audits covering ESG data integrity alongside traditional ISMS scope
- Supplier and third-party security requirements written into ESG supply chain contracts
- Incident response plans that specifically address ESG reporting disruption
- Integration with ISO 14001, ISO 45001, ISO 50001, ISO 22301, ISO 9001 via Integrated Management System (IMS)

Integrating ISO/IEC 27001

Integrated Management Systems (IMS) - The foundation of modern ESG governance

Most organizations don't need five separate management systems. They need one unified governance framework that covers quality, environmental impact, health & safety, energy, and information security simultaneously. This is what an Integrated Management System (IMS) delivers and it's where ERM CVS bring business value and improved performance.

An IMS consolidates ISO 9001, ISO 14001, ISO 45001, ISO 50001, ISO 22301 and ISO/IEC 27001 into a single Plan-Do-Check-Act framework. This means:

1

One set of audits covering all standards, not five separate certification cycles

2

One coherent governance structure accountable to the board - not fragmented compliance silos

3

One audit trail for ESG reporting, meeting CSRD, GRI, TCFD, and investor requirements with a single evidence base

4

One risk register integrating cyber, environmental, operational, and social risks

5

Faster certification, lower cost, and significantly reduced audit burden on your teams

Alongside ISO 27001, many organizations strengthen their broader digital resilience and governance posture by adopting complementary frameworks such as ISO 27701 for privacy management, ISO 27017 and ISO 27018 for cloud security and data protection, ISO 27019 for energy sector cybersecurity, and the NIST Cybersecurity Framework. These standards extend the scope of an ISO 27001 based ISMS, helping organizations address sector-specific risks, meet regulatory expectations, and enhance overall digital governance. Together, they create a more robust, resilient, and trustworthy information security ecosystem.

ISO/IEC 27001 also intersects closely with ISO 22301(Business Continuity) and ISO 42001 (Artificial Intelligence), creating a connected approach to digital resilience. ISO 22301 ensures that critical operations remain available during disruption, while ISO 42001 governs responsible and transparent AI use. Together, these standards complement an ISO 27001 based ISMS by linking information security, business continuity, and AI governance into one integrated, resilient framework that strengthens operational trust and reduces emerging technology risks.

Integrated management systems accelerate value by unifying governance, controls, and data across standards, enabling organizations to reduce duplication, strengthen decision making, streamline audits, and deliver faster, more consistent performance improvements.

Drive competence across cyber, ESG, and governance

Certification is only as strong as the people who operate the system. ERM CVS is certified by Exemplar Global across its ISO management system auditor programs, equipping your teams, security professionals, ESG leaders, and internal auditors with the competence to implement and audit ISO/IEC 27001 effectively. Our training builds the internal capability needed to run, maintain, and continually improve an Information Security Management System, with strong internal audit skills that help organizations assess ISMS performance, identify risks, strengthen controls, and stay ready for external certification audits. This can also be complemented with our modular program to upskill across other ISO management systems efficiently.

ISO 27001 Understanding

Ideal for ESG teams, sustainability managers, and anyone new to the standard who needs to understand how ISO 27001 protects ESG data

ISO 27001 Internal Auditor

Build in-house audit capability - train your own teams to verify ESG data controls, access management, and incident response

ISO 27001 Lead Auditor

Qualify to lead third-party and certification audits - for professionals building careers in ESG assurance and governance

Available online and in-person. Group and corporate training programmes can be tailored to your organization’s specific ESG governance, information security and integrated management system needs.

Why partner with ERM CVS?

We are sustainability and ESG specialists - not just cybersecurity auditors

ERM CVS provides independent assurance, certification, and training grounded in over 50 years of ERM's sustainability and governance expertise. Since 1996 we have helped organizations manage information, risk, and accountability in line with rising expectations for stronger digital and ESG governance. This heritage informs our ISO/IEC 27001 audits, where information integrity is central to credible sustainability and regulatory disclosures.

We certify a full suite of ESG linked management system standards, including ISO 14001, ISO 45001, ISO 50001, ISO 9001, and ISO 22301, enabling us to evaluate information security standalone or within your broader governance ecosystem. A breach of sustainability, operational, or human capital data can be as consequential as a financial breach, and our assessments reflect that.

Through our audits and training programs, we help organizations achieve ISO/IEC 27001 certification, strengthen internal controls, improve ESG data integrity, and build long term digital and operational resilience. ERM CVS is recognized by regulators, investors, and industry bodies for delivering rigorous assurance that supports credible governance and continual improvement.

How we support your ISO/IEC 27001 journey and deliver value beyond certification:

Integrate information security into business strategy:

ISO/IEC 27001 helps organizations embed information security into strategic direction, risk management, and operational planning. ERM CVS supports clients in integrating cyber risk, data governance, regulatory obligations, and secure by design principles into their ISMS in a practical and scalable way.

Benefit from expert-led audits and training:

Our auditors and trainers bring deep expertise in information security, digital governance, ESG data integrity, and sector specific regulatory expectations. This enables organizations to gain meaningful insight from audits and training, well beyond checklist based compliance.

Achieve operational impact:

Use ISO/IEC 27001 as a strategic tool to strengthen controls, reduce cyber incidents, protect ESG and operational data, manage third party and supply chain digital risks, and support stakeholder and regulatory expectations for trustworthy information handling.

Realize value beyond certification:

Certification is only the starting point. ERM CVS helps organizations leverage ISO/IEC 27001 to enhance governance maturity, strengthen digital and operational resilience, protect sustainability and regulatory data, and align information security with broader ESG and business commitments.

Find out more at ermcvs.com

Contact us to book a free consultation at post@ermcvs.com

ERMCVS

ERM CVS is an accredited UKAS certification body and ANAB accredited validation and verification body. We operate in accordance with recognized international assurance standards and are a certified training provider for ISO management systems.

ANAB ANSI National Accreditation Board ACCREDITED ISO 14065 VALIDATION AND VERIFICATION BODY

UKAS MANAGEMENT SYSTEMS 0067

EXEMPLAR GLOBAL