GLOBAL RISK REPORT

JS|HELD

2025


+91.02
-62.94
-1.03956
▲ 3.30790
▼ 1.93847
▲ 8.04968
▲ 7.39486
▼ 0.59367
-56.20
+49.02

INDEX

2025 J.S. HELD

G L O B A L R I S K R E P O R T

INTRODUCTION

The recommended focus for businesses in 2025 across the global landscape is **adaptation,** driven by political transitions, technological advancements, evolving operational risks, anticipated regulatory shifts, and changing economic conditions.

Through our work advising Fortune 100 companies, Global 200 law firms, top insurance companies, financial institutions, and government agencies—and understanding some of the most impactful topics on people's minds, along with the external factors expected to influence organizations—we have curated insights to help clients navigate risks and capitalize on emerging opportunities in the year ahead.

Topics covered in the 2025 J.S. Held Global Risk Report include:

1. Sustainability Investments & Headwinds
2. Global Supply Chain Challenges
3. The Rise of Crypto & Digital Assets
4. Artificial Intelligence, Data & Digital Regulations
5. Managing Cyber Risk

By providing greater clarity on these themes and their associated risks and opportunities, we will be partnering with clients to anticipate, adapt, and advance in 2025. If you have any questions or would like to further discuss the report, email **GlobalRiskReport@jsheld.com.**

1

SUSTAINABILITY

INVESTMENTS & HEADWINDS

Sustainability continues to be a hot issue around the world. While many jurisdictions are creating additional frameworks in support of greater consideration of sustainability, others, most notably the US, are either dragging their feet or even backsliding. When examining Environmental, Social, & Governance (ESG) regulations from different parts of the globe, new ESG regulations are creating a challenging backdrop for businesses and organizations as new compliance requirements, some of which may be conflicting, come into effect. Significant uncertainty will affect multinational companies selling into the EU market, driven by the EU's Corporate Sustainability Due Diligence Directive (CS3D). Adopted in 2024, CS3D requires EU and non-EU companies to conduct due diligence to identify and prevent adverse environmental and human rights impacts within their business and supply chain. Conflicts in climate-related reporting and disclosures requirements in different jurisdictions remain among the most significant challenges facing companies today. Meanwhile, in the US, the term "ESG" itself has become controversial, leading many to now refer more widely to sustainability and discuss ESG as the reporting component

New ESG regulations are creating a challenging backdrop for businesses and organizations as new compliance requirements, some of which maybe conflicting, come into effect.

of efforts under the broader banner. Several US states have mandated ESG criteria—including climate risk assessment—for investment decisions in state-related retirement funds, while other states have opposed such ESG considerations. Even so, organizations will need to be mindful according to overall sustainability practices since certain permits in many jurisdictions cannot be obtained without addressing environmental impact. With the arrival of the second Trump administration, environmental justice directives established by the Biden administration will be early targets for elimination, as well as grants and tax credits enacted for sustainability. Businesses can also expect closer judicial scrutiny in the wake of recent Supreme Court opinions, such as the *Loper Bright* ruling, which undercut agency authority to define regulatory compliance or noncompliance. The ruling will make challenges to sustainability and other environmental compliance regulatory programs more likely.

6 RISKS FOR SUSTAINABILITY INVESTMENTS & HEADWINDS

1

Regulations under the EU's Corporate Sustainability Due Diligence Directive (CS3D) as violations of the directive could result in fines and civil liability

2

A growing wave of regulations and litigation to combat greenwashing, the intentional or unintentional practice where exaggerated or false claims are made—or greenhushing, intentionally withholding or underreporting information—about the sustainability of a product, service, or company

3

US regulatory uncertainty, the pending US Securities and Exchange Commission's Climate Risk Disclosure rules for public companies (both domestic and foreign issuers filing annual reports with the SEC), which would require disclosure of:

- **A** Material climate-related risks
- **B** Activities to mitigate or adapt to such risks
- **C** Organizational leadership and board of directors' oversight of climate-related risks and management
- **D** Climate-related targets or goals that are material to the business, results of operations, or financial condition
- **E** In the end, these are likely targets for a second Trump administration to cut entirely or never finalize

4

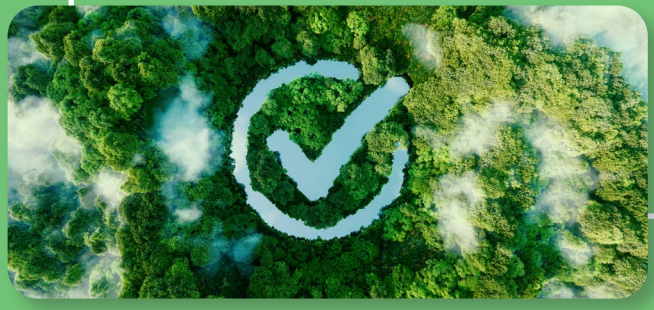
The SEC's reporting requirement of a company's Scope 1 and 2 greenhouse gas emissions on a phased-in basis by larger companies when emissions are material

5

Increased shareholder activism demanding more detailed insight into corporate sustainability goals

6

Litigation to enforce previous commitments to unwind downward revisions of commitments and disclosures, and to generally push goals that may not track with overall corporate strategy around sustainability



THE CORPORATE SUSTAINABILITY DUE DILIGENCE DIRECTIVE (CS3D) BROKEN DOWN

» **CS3D applies to three main groups:**

1. Companies in the EU with 1,000+ employees and EUR 450+ million global net turnover
2. Non-EU companies ("third-country companies") with EUR 450+ million net turnover in the EU
3. Companies that do not meet these specific thresholds but are a parent company of a group that does meet these requirements

» **Companies must apply their ESG due diligence policies to the following direct and indirect business partners in their supply chain:**

- Upstream business partners: Those related to the production of goods or provision of services, such as design and manufacturing
- Downstream business partners: Those related to distribution, transport, and storage of goods

» **Companies must comply starting with the largest in size in 2027, and continuing over the following two years with additional smaller-sized companies:**

2027

Companies with **5,000+** employees and **USD 1,500 million** turnover

2028

Companies with **3,000+** employees and **USD 900 million** turnover

2029

Companies with **1,000+** employees and **USD 450 million** turnover

ANTI-GREENWASHING & GREENHUSHING RULES TO WATCH FOR:

» EUROPEAN UNION

Enacted the Directive on Empowering Consumers for the Green Transition. Effective March 26, 2024, it is designed to eliminate deceptive environmental claims.

» UNITED KINGDOM

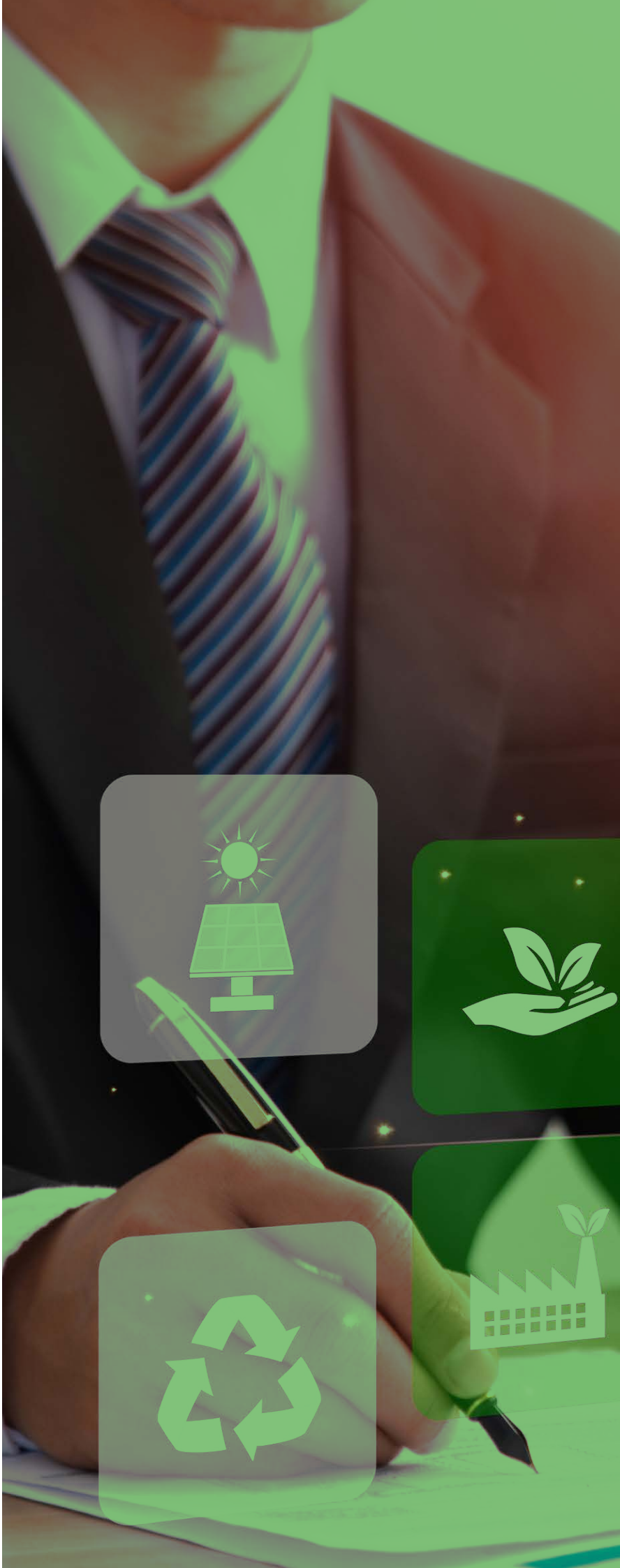
Revised guidelines for its Sustainability Disclosure Requirements (SDR), which focus on environmental advertising and emphasize the truthful marketing of a product's ecological advantages.

» UNITED STATES

The Federal Trade Commission (FTC) is revising its **"Guides to the Use of Environmental Marketing Claims," or "Green Guides,"** which advise on environmental marketing and how to substantiate claims to avoid consumer deception.

» 50 US STATES & THE DISTRICT OF COLUMBIA

Many have their own laws prohibiting deceptive practices, with some specifically enacting anti-greenwashing laws. Several consumer class actions have been brought in state courts.



OPPORTUNITIES TIED TO SUSTAINABILITY INVESTMENTS & HEADWINDS

1

Green funds – Backers are paying more attention to these investment vehicles that fund companies and projects focused on ESG issues

2

Companies with higher levels of ESG performance will continue to see a higher return on investment and less volatility in economic performance

3

Carbon technology start-ups are becoming an emerging sector with the US Inflation Reduction Act putting USD 800 billion into the commercialization of decarbonization solutions

Sub-sectors include:

- **Energy**
- **Climate adaptation**
- **Green fintech**
- **Carbon accounting and offsets**
- **Fundamental scientific research**

USD 619 BILLION

The total new global investment in renewable energy in 2023, up 8% from 2022 (USD 571 billion). In 2021, the number was USD 459.8 billion.

IN 2020, THE NUMBER WAS USD 372 BILLION.

(Source: Statista.com)

USD 3.36 TRILLION

Assets under management (AUM) of sustainable funds worldwide in 2023. In 2022, AUM was approximately

USD 2.8 TRILLION.

(Source: Statista.com)

59%

The number of C-suite executives surveyed in 2022 who said their organizations were using more sustainable materials, as well as increasing the efficiency of energy use.

(Source: Statista.com)

2,079

The number of companies worldwide in 2022 with approved science-based emission targets, almost double the amount reported one year earlier.

(Source: Statista.com)

82%

Percentage increase in consumer willingness to pay for sustainable packaging in 2023. That number soared from just a 4% increase in consumer willingness to pay more in 2022.

(Source: Statista.com)

80%

Approximate percentage of companies surveyed that have a Chief Sustainability Officer (CSO).

(Source: Forbes 2024 Sustainability Report)

USD 649 BILLION

The record amount of investment into ESG-focused funds by November 2021, up from USD 542 billion in 2020 and USD 285 billion in 2019.

10%

Percentage that ESG-focused investment funds now account for out of world-wide fund assets.

(Source: Reuters, based on data from Refinitiv Lipper)

65%

Percentage of executives surveyed who said sustainability ranks as a "top three" priority on the C-Suite agenda in 2024, up from 28% in 2021.

25%

Percentage of executives surveyed who ranked sustainability as the "number one" priority.

(Source: Forbes 2024 Sustainability Report)

75%

Percentage of those surveyed who said emerging technology will play a critical role in driving sustainability at their organization.

(Source: Forbes 2024 Sustainability Report)

27%

How much more confident companies with a CSO are about the positive impact of their sustainability initiatives than companies without a CSO.

25%

How much more confident leaders of organizations with a CSO are that their sustainability initiatives positively affect their bottom line and shareholder value.

(Source: Forbes 2024 Sustainability Report)

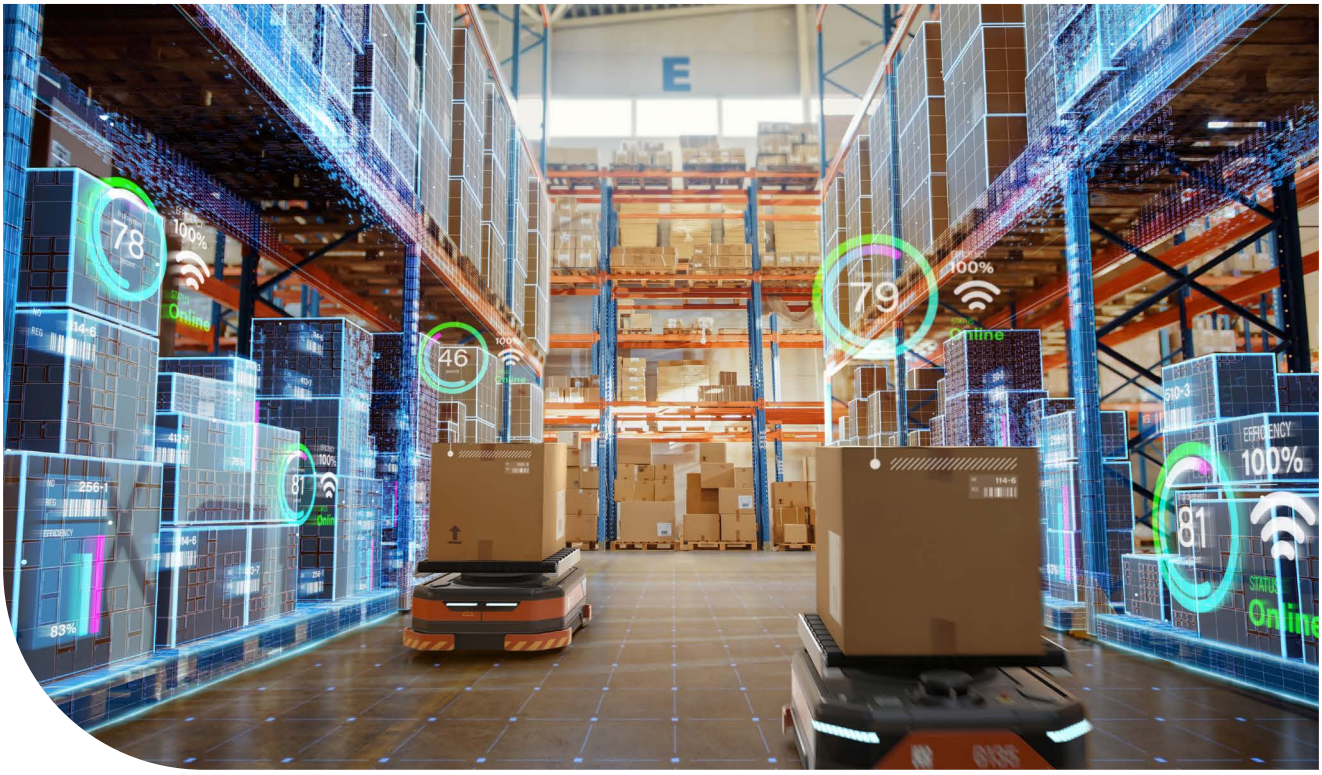
2

GLOBAL SUPPLY CHAIN

C H A L L E N G E S

The importance of the global supply chain has never been more apparent since the COVID-19 pandemic resulted in worldwide shortages of products and drove prices and inflation skyward. Supply chain disruptions have become the norm, attributable to an array of modern-day events and conditions including climate change, natural disasters, cyberattacks, fraud, or geopolitical instability, such as conflict in the Middle East or the Russia-Ukraine war. Gone are the days when companies could blame production problems on their suppliers and not take responsibility. Increased globalization from the interconnectedness of companies makes them and their supply chain more vulnerable, ranging from cyber incidents caused by internet proliferation to basic material shortages. Further, customers are demanding to know where a company's products come from, how they are sourced, how they are manufactured, and if any part of the process has a deleterious effect on people or the environment. Governments have responded by enacting new rules and regulations, or enforcing older ones, to ensure supply chain accountability is a major priority for companies in every industry. This is true especially within the European Union, where individual member-states have enacted protective legislation and rules. As consumers, governments, and corporations acknowledge the effects of supply chain risks, transparency and due diligence will become more critical to the internal compliance structure of global businesses. The enactment and greater enforcement of laws focused on sustainability issues have increased the obligations on companies to examine the sources and actions of their suppliers and how it all impacts the entire value chain.

Customers are demanding to know where a company's products come from, how they are sourced, how they are manufactured, and if any part of the process has a deleterious effect on people or the environment.



8 RISKS FOR GLOBAL SUPPLY CHAIN

1

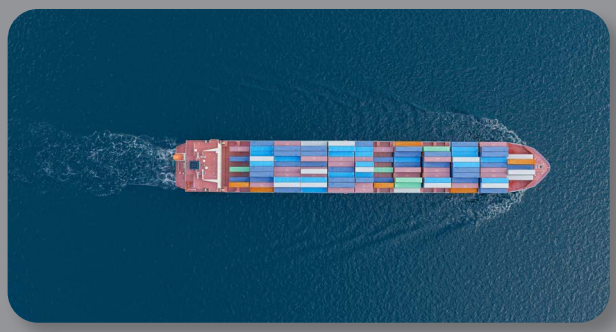
Geopolitical risks in the Middle East between Israel and Hamas; the ongoing war between Russia and Ukraine; and anticipation of tougher sanctions

2

Natural disasters and extreme weather events

3

Disruptions in key routes—such as the Suez Canal, Panama Canal, and Red Sea—increasing freight rate volatility



4

A patchwork of laws, rules, and regulations that vary by jurisdiction, such as:

- **A** The EU Corporate Sustainability Due Diligence Directive (CS3D)
- **B** The EU Corporate Sustainability Reporting Directive (CSRD)
- **C** The Supply Chain Act
- **D** The UK Economic Crime and Corporate Transparency Act
- **E** The UK Modern Slavery Act
- **F** Australia's Modern Slavery Act
- **G** Canada's Fighting Against Forced Labour and Child Labour in Supply Chains Act
- **H** The UK Bribery Act, US Foreign Corrupt Practices Act, Canada's Corruption of Foreign Public Officials Act, Australia's criminal code addressing anti-bribery, plus a multitude of countries in the Asia-Pacific where private sector bribery and / or bribery of foreign public officials is illegal
- **I** Germany's Supply Chain Duty Act
- **J** Anti-Greenwashing regulations updated in the EU and UK, including:
  1. The Directive on Empowering Consumers for the Green Transition
  2. The Corporate Sustainability Reporting Directive (CSRD)
  3. The Sustainability Disclosure Requirements (SDR)
  4. Revised guidelines from the UK's Financial Conduct Authority
- **K** The EU Deforestation Regulation (EUDR), which covers seven commodities—cattle, cocoa, coffee, palm oil, rubber, soy, and wood—with enforcement likely to begin late 2025
- **L** Greater enforcement of the Uyghur Forced Labor Prevention Act (UFLPA), preventing goods produced in China's Xinjiang Uyghur region from entering the US

5

Cyber threats / cyberattacks on third-party suppliers or vendors in the supply chain

6

Second Trump administration's proposed US tariff increases, which could result in retaliatory counteractions by affected exporters to the US and other trade partners. Proposed tariff amounts include:

- **A** 10% to 20% on all imports
- **B** 25% to 50% on Chinese semiconductor chips
- **C** 60% or higher on all other goods coming from China

7

Dependence on critical minerals, materials, and rare earths that are mined and imported from geopolitically risky locations and jurisdictions with which relations are strained or hostile

8

Financial leakage through deliberate overstatement of pricing and costs, lack of policing, and control of contractual supply chain terms

GLOBAL **SUPPLY CHAIN OPPORTUNITIES**

Transparency and traceability via block-chain and other automated mechanisms

Greater use of advanced technologies in the supply chain can result in lower logistics costs with better tracking and monitoring of goods

Reshoring and nearshoring depending on the industry—in the US, for example, under the CHIPS and Science Act's semiconductor provisions, some production of leading logic and memory chip manufacturing will be brought back into the country

Companies incorporating sustainable, ethical, and legally compliant supply chain strategies will gain a competitive edge due to improved reputation among consumers

Providers within the Supply Chain as a Service (SCaaS) market, which includes the outsourcing of supply chain management (i.e., warehouse, logistics, and supplier / vendor management) will see large growth

Greater diversity within supply chains by adding more locations and suppliers

Innovations for finding replacements and alternatives for product supply chains are evolving and can lower the cost of production

Data accessibility allows all parties within a supply chain to have access and use real-time information to help with scheduling, finding optimal routes, lowering costs, and improving traceability to pinpoint and resolve problems quickly

USD 184 BILLION

Annual cost of global supply chain disruptions for organizations.

(Source: Swiss Re)

76%

Percentage of the 2,000 European shipping customers of logistics giant Maersk who said they have experienced supply chain disruptions causing delays to their business in the past year.

22%

Percentage of those customers surveyed who counted more than 20 disruptive incidents during the same period.

(Source: Maersk)

USD 81.93 BILLION

Projected value of the global supply chain management market in 2033, rising from USD 31.77 billion in 2024 and an estimated USD 35.30 billion in 2025.

(Source: Precedence Research)

USD 23.84 BILLION

Projected value of the US supply chain management market in 2033, rising from USD 8.81 billion in 2024 and an estimated USD 9.84 billion in 2025.

(Source: Precedence Research)

USD 138 BILLION

Predicted global annual cost of software supply chain attacks to businesses in the year 2031, up from an estimated USD 60 billion expected in 2025.

(Source: Cybersecurity Ventures)

USD 7.9 BILLION

Amount the Supply Chain as a Service (SCaaS) market is expected to reach in 2025, up from USD 4.5 billion in 2017.

(Source: Allied Market Research)

USD 157.6 BILLION

Projected value of artificial intelligence in the global supply chain by the end of 2033, up from USD 4.5 billion in 2023.

(Source: market.us/scoop)

3

THE RISE OF CRYPTO

& DIGITAL ASSETS

While the cryptocurrency industry is still relatively young, its adoption by various economic sectors and the evolution of the technology itself is growing, along with the tokenization of assets, AI-powered smart contracts, and decentralized finance (DeFi) becoming more accessible to customers. Yet, with all the hype and opportunity surrounding crypto, concerns over security, volatility, and regulatory scrutiny are increasing as well. Companies in every sector are looking at the use of crypto to gain an advantage. Even the gaming industry has entered the crypto space with bridging services offering "Play-to-Earn" games. Anonymity is a key feature in both the risk and success of cryptocurrency. The concept of "Know Your Customer" on centralized platforms is still required, but anonymity attracts some participants to DeFi platforms who want to transact on a peer-to-peer level without a third party. Anonymity is also prompting criminals to use virtual currencies to conduct illicit activities and conceal their profits. Other concerns still looming for governments include crypto asset company bankruptcies and the 2022 failure of the FTX crypto exchange.

Companies in every sector are looking at the use of crypto to gain an advantage.

In the US, with the new Trump administration's pro-crypto position, there will likely be a shift from the previously restrictive policies which the Securities & Exchange Commission had been enforcing. Many are hoping for a regulatory reset as well as more clearly defined regulation that will spur innovation and allow companies to blossom. The EU has moved further along in regulating crypto, enacting regulations on the transfer of crypto assets in an effort to deter money-laundering. The EU's Markets in Crypto-Assets (MiCA) law requires any company issuing or trading crypto to obtain a license. Starting in 2026, MiCA will also require crypto asset service providers to collect information about the sender and beneficiary of transfers. The UK requires any company offering cryptocurrency to obtain authorization from the nation's Financial Conduct Authority. China has banned cryptocurrency trading and mining outright, while both Japan and Canada require crypto companies to register with their governments and abide by anti-money laundering laws. With all that said, risk and legal uncertainties abound since crypto is classified differently depending on the regulatory agency.

6 CRYPTO & DIGITAL ASSETS **RISKS**

1

Increasing investigation by regulators into potential fraud, based on complaints received by various agencies around the globe

2

Environmental scrutiny over the massive energy usage of crypto mining

3

Market volatility after the halving of bitcoin in 2024, which can reduce the block reward by 50%, lower the supply of bitcoin, and result in a price increase (the next halving occurs in 2028)

4

Sanctioned countries using cryptocurrencies to circumvent Western sanctions—for example:

- **A** Russia
- **B** Iran
- **C** North Korea
- **D** Venezuela

5

Manipulation of tokens resulting in the collapse of coin value—for example:

- **A** Terra LUNA case – saw a loss of more than USD 40 billion in one day

6

Cryptocurrency being used as payment for criminal activity and to conceal illegal financial activity—for example, it is often used for payment in:

- **A** Ransomware cases
- **B** Money laundering cases
- **C** Terrorist financing

CRYPTO & DIGITAL ASSETS **OPPORTUNITIES**

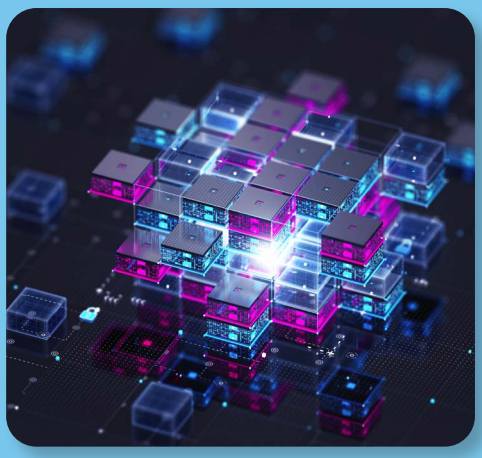
1

The adoption of crypto among the gaming and entertainment industry

2

Increasing use of crypto ledgers and blockchain technology to itemize movements through various industry supply chains is improving:

- **A** Traceability
- **B** Transparency
- **C** Efficiency
- **D** Speed
- **E** Security



3

Investment in compliance systems and processes because of greater regulatory scrutiny to come

4

Educational programs on crypto for consumers translates into greater investment in crypto assets

5

Companies that can investigate and trace the anonymous controllers of wallets may see growing engagement

6

Use of crypto platforms as a safety net to store personal identity information of people displaced by war and similar conflicts

USD 3.4 TRILLION

Total amount the global crypto market capitalization has reached in November 2024.

USD 108,268

Record high set by bitcoin, with a market capitalization reaching USD 2.1 trillion in December 2024.

(Sources: Coingecko.com and Coinmarketcap.com)

USD 4.6 BILLION

Blockchain gaming market size as per revenue in 2022.

USD 65.7 BILLION

Amount the blockchain gaming market is expected to reach in 2027.

(Source: MarketsandMarkets Analysis)

87 TO 91 TERAWATT-HOURS (TWH)

Bitcoin's annual energy consumption range, which is more than the country of Finland uses.

107.30 MILLION

The number of projected users in the cryptocurrency market by 2025.

(Source: Statista)

63%

Percentage of Americans who say they have little or no confidence that cryptocurrencies are reliable and safe.

(Source: Pew Research Center)

69,000

The number of complaints from the public received by the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) in 2023 regarding financial fraud involving the use of cryptocurrency, such as bitcoin, ether, or tether.

USD 5.6 billion: Total estimated losses with a nexus to cryptocurrency.

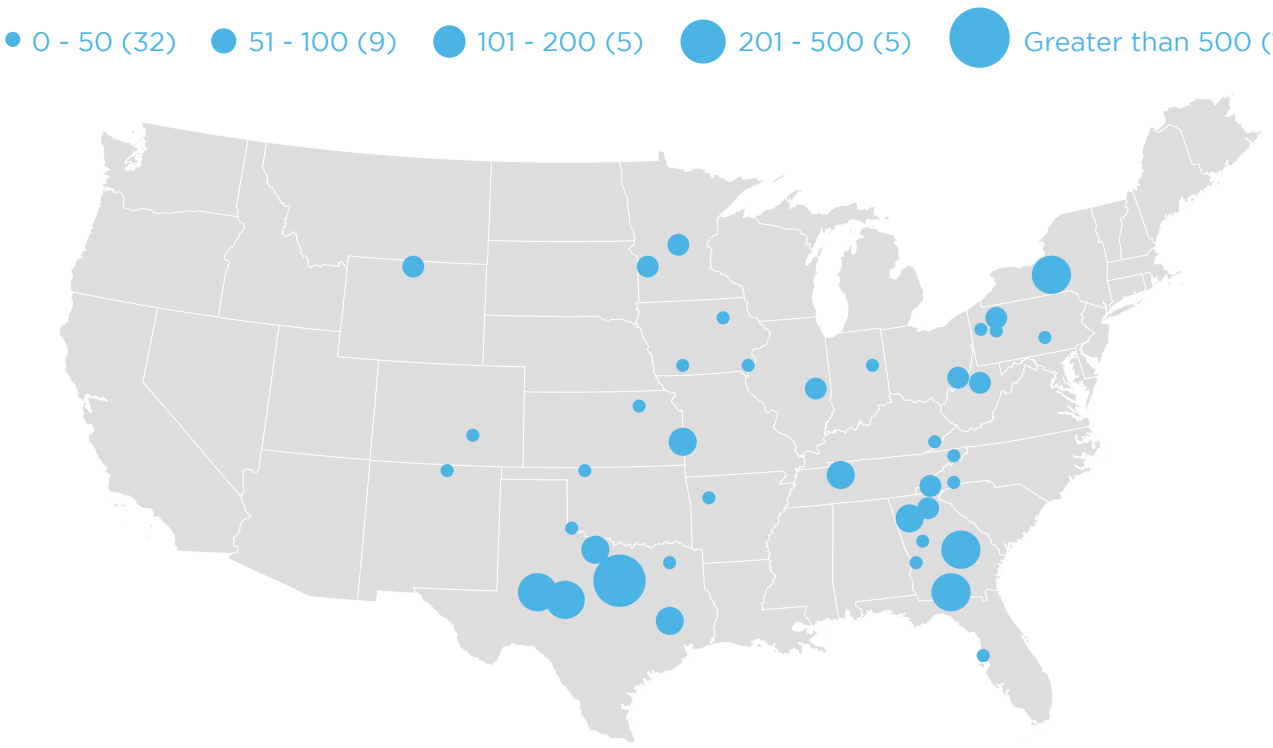
(Source: FBI Cryptocurrency Fraud Report)

CRYPTO MINING ELECTRICITY / ENERGY USAGE IN THE US

Locations of 52 US cryptocurrency mining operations as of January 2024.

(Source: US Energy Information Administration – see map below)

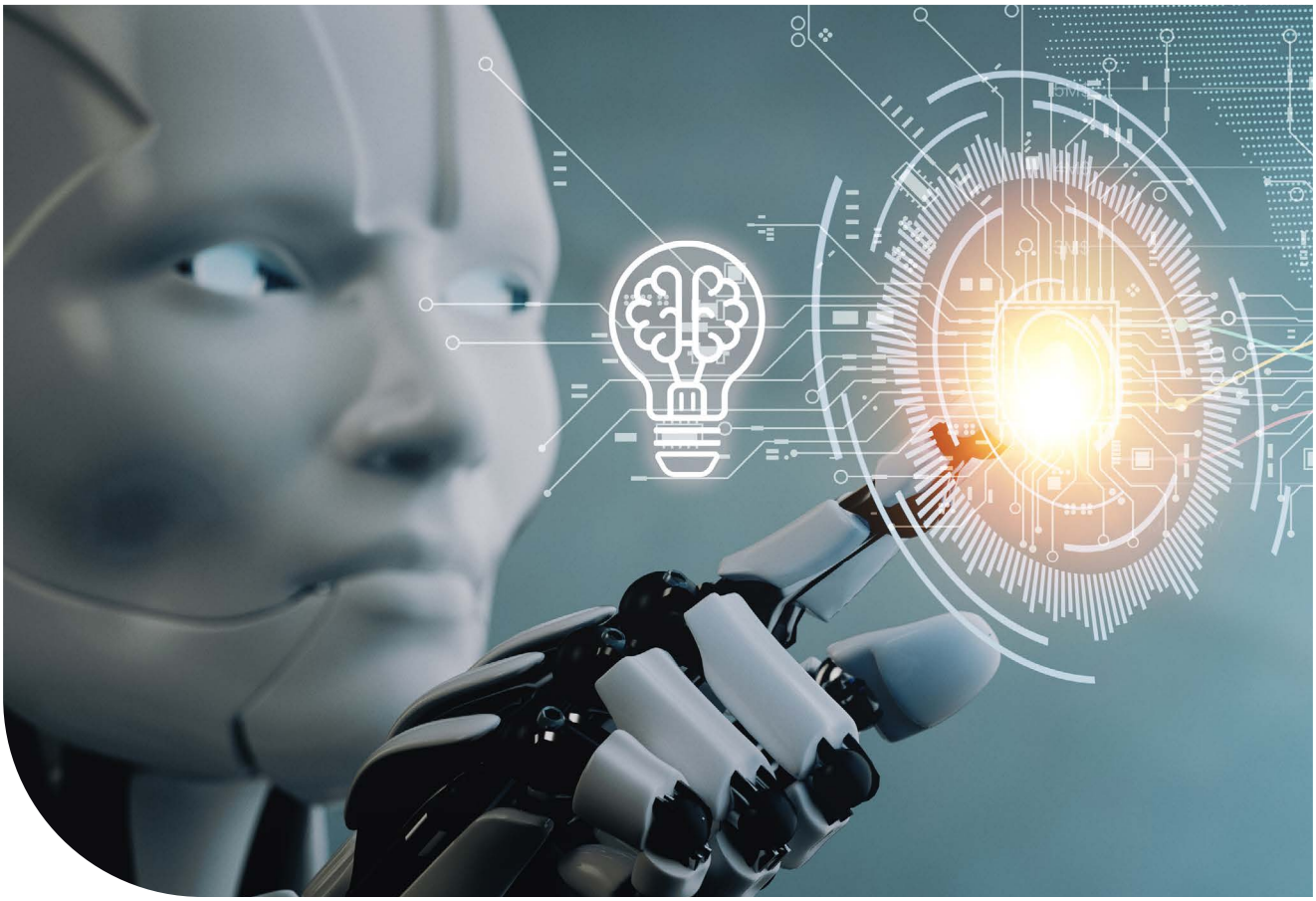
Cryptocurrency mining facilities by existing capacity in megawatts (MW)



4

ARTIFICIAL INTELLIGENCE,

DATA & DIGITAL REGULATIONS



Artificial Intelligence (AI) has been touted as the answer to a multitude of business challenges. However, AI—along with machine learning and large language models (LLMs)—is still fraught with technical and regulatory challenges as the technology evolves. Threat actors use AI to create deepfake videos, text, and audio; craft convincing phishing emails; bypass security measures; and automate malicious activities—prompting national and international security concerns. Companies are developing their own Generative AI (GenAI) models to improve efficiency and boost their bottom line. However, GenAI algorithms demand massive amounts of data to train the system, which means using vast datasets from diverse sources, resulting in privacy and copyright concerns over data collection.

In response, governments are proposing and / or enacting new laws and regulations to prevent or mitigate harm that AI usage may cause. For example, new regulations in Europe are designed to protect fundamental rights, including privacy of consumers' personal information, as well as other justice and ethics issues. While that may put the region at a competitive disadvantage due to increased reporting burdens on companies, it also clarifies obligations and reduces the burden of trying to harmonize varying rules. Despite such issues, companies seeking to build an AI framework need to realize that with more data comes more risk, and proper risk protocols should be in place to help ensure privacy, security, and consideration of the wider Environmental, Social, and Governance (ESG) policies that each organization has put into place.

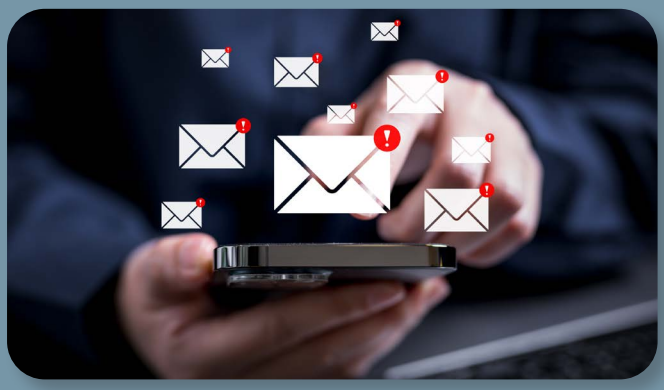
Companies are developing their own Generative AI (GenAI) models to improve efficiency and boost their bottom line.

10 RISKS FACING ARTIFICIAL INTELLIGENCE, DATA & DIGITAL REGULATIONS

1

Cyberattacks and malware powered by AI, potentially resulting in:

- **A** Data breaches
- **B** Theft of personal information or intellectual property
- **C** Disruption of services
- **D** Increased costs



2

Data poisoning – when an attacker changes the behavior of a GenAI system through manipulation of its training data or process, potentially jeopardizing the reliability of that GenAI model

3

Disinformation litigation — output based on biased data and hallucinations (incorrect or misleading results) may subject the operator to legal risks

4

The EU's Artificial Intelligence Act, which imposes significant responsibility and risk management requirements on companies that provide high-risk AI systems, such as:

- **A** Critical infrastructure operations
- **B** Automated insurance claims processing
- **C** Credit scoring
- **D** Systems for hiring or evaluating employees

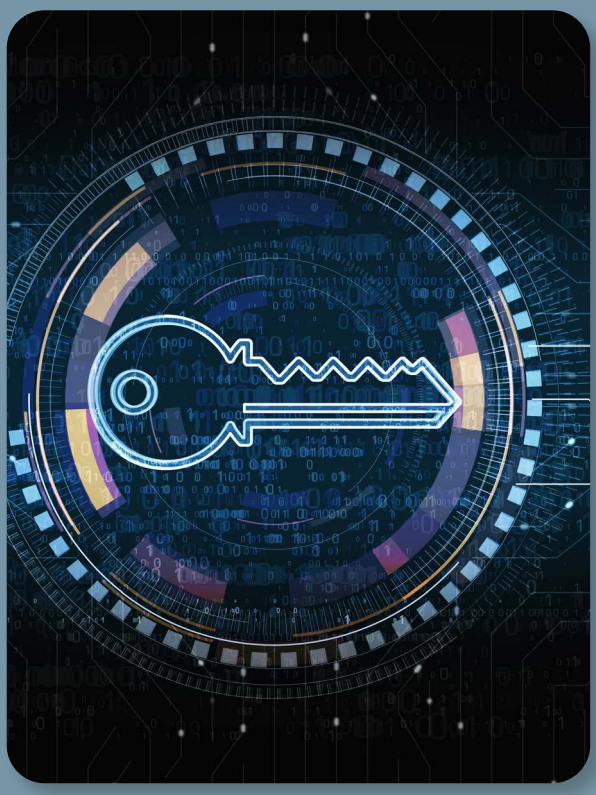
5

Data being used to train a company's LLM may be covered by copyright and could lead to intellectual property (IP) litigation

6

AI is expensive due to cybersecurity certification and enormous energy consumption

7



M&A transactions – when acquiring a company with an AI framework, the acquirer needs to ask:

- **A** What data is being inherited?
- **B** What type of vetting will be conducted?

8

Environmental impact of AI, due to factors such as:

- **A** AI being housed in data centers that generate electronic waste containing hazardous substances
- **B** Data centers relying on water during construction and later to cool electrical components
- **C** Data centers requiring energy that often comes from burning fossil fuels
- **D** Microchips used by AI needing rare earth elements that are not always mined according to ESG standards

9

Not building an AI system may mean losing a competitive advantage—conversely, putting an AI product out too quickly may open up a whole new vector of vulnerabilities for cyberattacks

10

Ethical problems with AI – the technology can be used to spread disinformation and create deepfakes and other synthetic media that could result in unintended plagiarism or produce false or abusive content

THE EU ARTIFICIAL INTELLIGENCE ACT CLASSIFIES AI ACCORDING TO ITS RISK

» **Unacceptable risk AI systems are prohibited in Article 5 of the Act.**

- This includes social scoring systems; use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques; use of an AI system that creates or expands facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage; and the use of biometric categorization systems to infer race, political opinions, religious beliefs, etc.
- Companies involved in prohibited AI systems face fines of up to EUR 35 million or 7% of global turnover.

» **Limited risk AI systems are subject to lighter transparency obligations.**

- Developers and deployers in this category must ensure end-users are aware they are interacting with AI (chatbots and deepfakes).
- Violations may result in fines of EUR 15 million or 3% of turnover.

» **Minimal risk AI systems, such as AI-enabled video games and spam filters, are unregulated.**

USD 400,000

The amount two investment firms agreed to pay in total civil penalties to settle charges brought by the SEC against two investment advisors for making false and misleading statements about their purported use of AI.

(Source: Sec.gov)

9% OF AMERICANS

feel confident in their ability to spot deepfake videos or recognize AI-generated audio, such as fake renditions of IRS agents.

(Source: McAfee | Tax Scams Study 2024)

AI, DATA & DIGITAL REGULATIONS **OPPORTUNITIES**

1. Speed of processing vast amounts of data and analyzing it quickly (i.e., automating repetitive tasks) is enabling organizational efficiency across industries

2. The use of AI for enhanced fraud detection by identifying patterns and anomalies in financial data is leading to faster response by cybersecurity, financial crime, and corporate investigations teams

3. Insurance policies are on the rise for AI risks covering data poisoning, usage rights infringements, and violations of regulations such as the EU's AI Act

4. AI in legal technology—for legal research, contract management, writing assistance, eDiscovery in litigation—is creating cost efficiencies by replacing human effort with AI computing

5. Larger AI companies are teaming with the nuclear energy sector to use small modular reactors (SMRs) to fulfill power needs for their massive data centers

6. Increased employment for people who can vet or review any final AI-generated product

63% OF BUSINESSES

have limited what data can be entered into GenAI tools, while 61% have limits on which employees can use them.

(Source: Cisco 2024 Data Privacy Benchmark Study | February 2024)

91% OF ORGANIZATIONS

recognize they need to do more to reassure customers their personal information is being utilized only for legitimate and intended purposes in AI.

(Source: Cisco 2024 Data Privacy Benchmark Study | February 2024)

5

MANAGING CYBER RISK

Cyber incidents such as the 2024 event involving Change Healthcare, which compromised the personal information of over 100 million people, highlight the evolving nature of cyber threats—increasingly becoming risk management challenges driven by disruptive new technologies, including AI. Such incidents can halt operations, prompt regulatory investigations, and result in significant financial costs. They often lead to increased insurance claims, litigation from affected parties, and even open the door for further issues like fraud. The Change case also underscores the steady rise in both the number and severity of cyberattacks and data breaches. In response to these trends, regulators and legislators, such as the US Securities and Exchange Commission (SEC) and European Union, have sought to enact new laws and regulations protecting consumers, patients, and investors. While the threats continue to evolve and new laws are drafted, organizations are fighting back by enacting stronger controls as part of new minimum cybersecurity thresholds mandated by common protection frameworks, such as the one outlined by the National Institute of Standards and Technology (NIST) in the US. Another key question around this topic: whether or not to pay a ransom. While companies should be asking their insurer if payment would be covered by their policy, paying a ransom could also inadvertently put a company in legal jeopardy—for example, by violating sanctions policies of the US Office of Foreign Assets Control. All told, the onus is on organizations to act proactively by establishing an information security and incident response program, having proper backup and protocols in place, and maintaining a deep understanding of what their cyber insurance covers for data breaches and other cyberattacks.

While the threats continue to evolve, and new laws are drafted, organizations are fighting back by enacting stronger controls as part of new minimum cybersecurity thresholds mandated by common protection frameworks.

5 CYBER RISK

1

Disruption of business due to a cyber incident

2

Litigation and/or reputational damage resulting from a cyber incident

3

Loss of sensitive data

4

Growing regulatory and legislative pressures in the US and Europe, including:

- **A** The EU's Network and Information Systems Directive 2 (NIS2) to improve cybersecurity in essential sectors (i.e., energy, transportation, banking, health, drinking water, digital infrastructure)
- **B** The EU's Cyber Resilience Act
- **C** The US Securities and Exchange Commission's cybersecurity disclosure rules
- **D** The US Transportation Security Administration's proposed rule mandating cyber risk management and reporting requirements for certain transportation owners and operators
- **E** The EU's General Data Protection Regulation (GDPR)

5

Not having the correct level of cyber insurance coverage—questions to ask include:

- **A** Does the company's cyberattack policy insure against ransomware or require separate coverage?
- **B** Is the insurance suitable for the company's industry and the data held?
- **C** Are there exclusions in the policy that limit liability if the company is in breach of compliance laws?
- **D** Are breach notification costs covered?

CYBER OPPORTUNITIES

1

Companies that adapt to incorporate stronger cybersecurity controls—such as Multi-Factor Authentication (MFA), advanced Endpoint Protection and Response (EDR), and immutable backup strategies and response planning—will aid insurance underwriting and meeting the requirements of external partners

2

Companies are using artificial intelligence to identify patterns and anomalies in data, therefore detecting fraud and cyberattacks more quickly and reducing costs

3

Insurance companies are seeing greater demand for cybersecurity and ransomware coverage from organizations in all sectors – however, some carriers are putting more exclusionary clauses into contracts

4

Companies using dependency mapping of different processes and assets will lessen the impacts of a potential cyber incident

5

Organizations with strong business continuity plans and cyber hygiene may receive better cyber insurance rates

A CLOSER LOOK AT CYBER REGULATIONS

» **The EU Cyber Resilience Act (CRA),** enacted in October 2024, imposes mandatory cybersecurity requirements for manufacturers and retailers of products that contain a digital component.

» **The US Securities and Exchange Commission's cybersecurity disclosure** rules went into effect at the end of 2023. Yet, companies are still grappling with the requirement that they disclose material cybersecurity incidents within four business days of discovery. The question of what types of incidents are considered "material" is still at issue. Additionally, publicly traded companies are required to make annual disclosures about their cybersecurity risk management, strategy, and governance.

» **Proposed rule from the US Transportation Security Administration** would mandate cyber risk management and reporting requirements for certain pipeline and rail owner / operators, and a more limited requirement for certain over-the-road bus (OTRB) owner / operators, to report cybersecurity incidents.

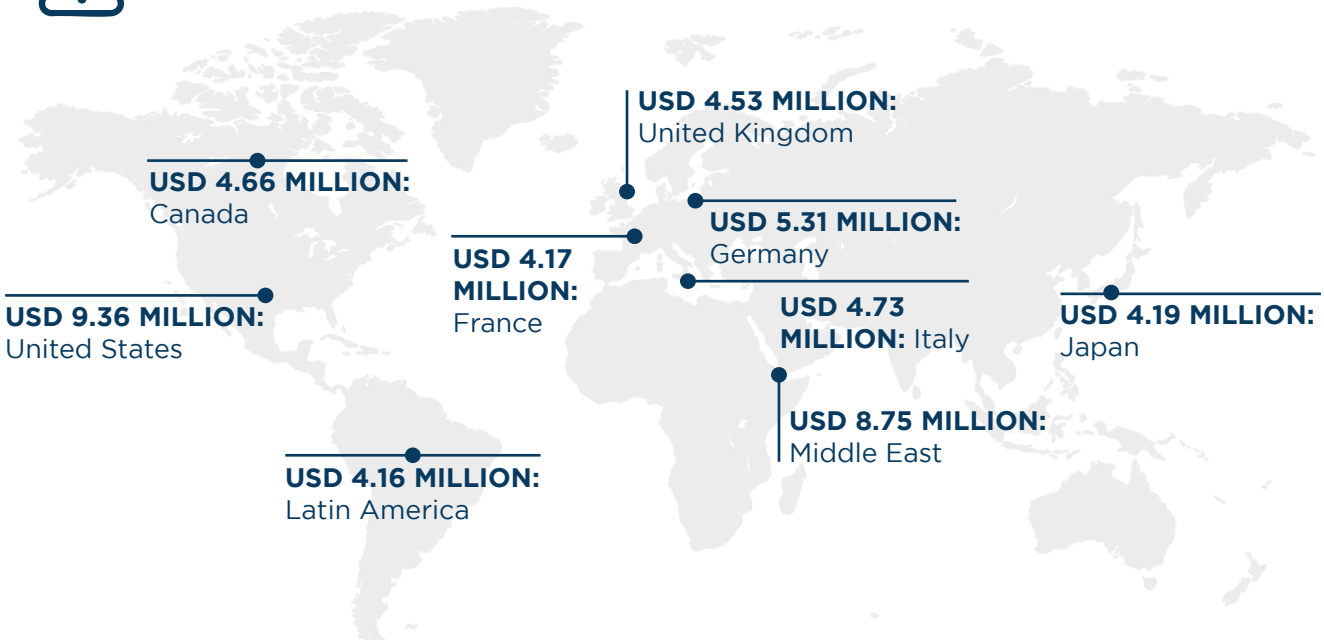
» **The EU's General Data Protection Regulation (GDPR)** governs the collection, use, transmission, and security of data collected from residents of the EU. Among the most significant requirements is that people must be allowed to give explicit consent before their personal data is collected. Fines of up to EUR 20 million or 4% of total global turnover may be imposed on organizations that fail to comply.

AVERAGE COST OF A DATA BREACH BY INDUSTRY WORLDWIDE FROM MARCH 2023 TO FEBRUARY 2024:

(Source: Statista.com)

- **USD 9.7 MILLION:** Healthcare
- **USD 6.08 MILLION:** Financial
- **USD 5.56 MILLION:** Industrial
- **USD 5.45 MILLION:** Technology
- **USD 5.29 MILLION:** Energy
- **USD 5.1 MILLION:** Pharmaceuticals
- **USD 5.08 MILLION:** Professional Services
- **USD 4.43 MILLION:** Transportation
- **USD 4.09 MILLION:** Communications
- **USD 4.09 MILLION:** Entertainment
- **USD 3.94 MILLION:** Media
- **USD 3.91 MILLION:** Consumer Products & Services
- **USD 3.82 MILLION:** Hospitality
- **USD 3.5 MILLION:** Education
- **USD 3.48 MILLION:** Retail
- **USD 2.55 MILLION:** Public Sector

COST OF A DATA BREACH BY COUNTRY OR REGION IN 2024:



(Source: IBM, Cost of Data Breach Report 2024)

1,320

The number of data breach class actions filed in the US in 2023, up from 604 filed in 2022 and 310 in 2021. The top 10 data breach settlements in 2023 totaled USD 515.75 million.

(Source: Duane Morris Class Action Review - 2024: A Comprehensive Analysis of Class Action Litigation)

USD 22 BILLION

The size of the global cyber insurance market expected by 2025. It will reach USD 29 billion by 2027 and exceed USD 130 billion by 2033.

(Source: Statista.com and SphericalInsights.com)

59%

Amount the US cyber insurance market accounts for of the USD 16.66 billion in premium written for cyber coverages globally in 2023.

(Source: NAIC – National Association of Insurance Commissioners)

USD 9.84 BILLION

of direct written premium (DWP) in the US was reported for cyber insurance coverage.

(Source: NAIC – National Association of Insurance Commissioners)

24 DAYS

The average disruption time a company suffers after a ransomware attack.

(Source: Statista.com)

USD 2.73 MILLION

The average ransomware cost in 2024, up from USD 1 million in 2023.

(Source: Sophos)

We would like to thank our colleagues for providing insights and expertise that greatly assisted this research.

This communication may contain forward-looking statements. These statements are based on J.S. Held's current expectations and are subject to risks, uncertainties, and other factors that could cause actual results to differ materially from those expressed or implied by such forward-looking statements. Forward-looking statements speak only as of the date they are made, and we undertake no obligation to update or revise any forward-looking statements, whether as a result of new information, future events, or otherwise. This material is for informational purposes only and is provided 'as is' without any warranties and J.S. Held assumes no liability for errors, omissions, or any actions taken based on this material.

JS|HELD

Find your expert.

2025