Transparency as Discipline

Sustainability Report 2025



GROUP-IB

Table of Contents

From the Management Team 03
About this Report 04
Group-IB at a Glance 05
Cybersecurity 11
ESG Strategy 16
Environment and Climate 22
Social 24
Governance 32
Appendices 36



In 2025, cybersecurity manifested itself not only in cyberspace but, more evidently than ever, in physical infrastructure — in hospitals, in power grids, in payment systems, and in the supply chains that move both goods and trust. Defending the digital domain has become an integral part of how societies build resilience, and it is no longer a discipline that can be cleanly separated from the broader work of keeping critical systems running.

Combined with the rapid rise of AI, this places a specific responsibility on companies like ours: to find the right balance between being at the forefront of research and development, and using AI responsibly and sensibly to preserve both sensitive data and the planet's resources. The same model that helps a defender act faster can help an attacker scale further. The same compute that powers our detection products consumes energy. Holding both truths in view is the defining test of leadership in our sector right now.

Our operational impact continued at scale: 1,809 cybercriminals were arrested, roughly USD 2.7 billion in phishing losses were prevented, around 65 million people were protected, and 34,838 pieces of malicious infrastructure were dismantled.

We also expanded the operational footprint and discipline that underwrites this work. Group-IB now maintains a presence across eight jurisdictions in Europe, META, Central Asia, the Asia-Pacific, and Latin America, with Digital Crime Resistance Centers in eleven countries, giving us proximity to the threats and the institutions we serve. Our team grew by more than a quarter since 2024, with 556 employees from more than 30 countries forming the backbone of the company.

We are proud to present this 2025 Group-IB Sustainability Report, in which we openly share our progress toward our Environmental, Social, and Governance goals, as well as the challenges we are working through to meet them.

Dmitry Volkov
CEO and Co-Founder, Group-IB



Digital security and sustainability are not separate disciplines — together, they contribute towards and strengthen societal resilience. The events of the past year reinforced what we have long believed at Group-IB: that the integrity of an organization is tested not at the moment of opportunity, but at the moment of disruption, and that the systems we build to withstand cyber threats are the same systems that allow our clients, our partners, and our communities to keep delivering on their own commitments. Sustainability, in our work, is not a parallel agenda. It is the result of operating well, consistently, and under pressure.

Our 2025 Sustainability Report is an effort not only to disclose and share our contributions towards sustainability, but also to understand our position more clearly and to set our ambitions responsibly in light of the fast-developing opportunities and risks represented by AI. We approach this with two convictions. The first is that transparency is itself a form of operational discipline: a company that can account for its data, its energy, its people, and its decisions is a company that can be trusted with sensitive information. The second is that responsible ambition must be matched to capability. We are choosing the targets we can defend, scaling the methodologies we can stand behind, and saying so plainly when work is still in progress.

Furthermore, this is the year in which we have moved from baseline to structure. We have published our new Code of Conduct and ensured that both internal and external stakeholders are aligned with it. We are moving forward toward the goals set in 2024, and we are introducing a formal approach to responsible AI that will continue to evolve alongside regulations and our own product portfolio. There is, of course, work to be done. This includes managing the resource consumption associated with our fast-growing business and technology development, as well as advancing the diversity of our governance bodies, which we have placed on record.

Thank you to our teams, our clients and partners globally who hold us to high standards, and to the colleagues whose daily work makes the numbers in this report real. While 2024 was the promise, 2025 is the proof and the commitment we carry forward.

Anastasiia Komissarova
Deputy CEO, Group-IB

About this Report

Group-IB presents its second annual Sustainability Report, covering the calendar year from 1 January to 31 December 2025. This section sets out the basis on which the Report has been prepared — the entities and activities it covers, the reporting frameworks applied, the methodological choices behind the data, and the regulatory landscape within which Group-IB operates — so that readers have a clear view of both the scope and the limits of what is disclosed here.

Reporting Entity and Boundary

This Report is prepared on a consolidated basis for Group-IB Global Private Limited (Singapore), the group's ultimate parent company, together with its regional entities and Digital Crime Resistance Centers across Europe, META, Central and Southeast Asia, and Latin America. Environmental data is consolidated on an operational-control basis.

The complete list of legal entities within the reporting boundary, and the treatment of leased and shared facilities, are disclosed in the Appendices.

Reporting Period

The reporting period is 1 January to 31 December 2025. Unless otherwise stated, all figures relate to the 2025 calendar year, with 2024 presented as the comparative baseline established in our inaugural Sustainability Report.

Reporting Frameworks

Group-IB reports voluntarily. Greenhouse gas emissions are calculated in accordance with the GHG Protocol Corporate Accounting and Reporting Standard. This Report is additionally prepared with reference to the GRI Standards as its primary disclosure framework, with climate-related information informed by the ISSB Standards (IFRS S1 and S2) and the TCFD recommendations, and material topics mapped to the relevant UN Sustainable Development Goals — subject to management confirmation of the framework(s) to be formally adopted. Where a disclosure aligns with a specific standard, this is indicated in the relevant section.

Basis of Preparation, Restatements, and Assurance

To improve precision, in 2025 we refined our emission factors — transitioning from BEIS datasets to national grid and regional sources where available — and applied an inflation control to spend-based Scope 3 categories. These changes and their effect on year-on-year comparability are described in the Environment and Climate section. This Report has not been externally assured. Group-IB keeps the case for independent limited assurance under review as its disclosure practice matures.

Regulatory and Reporting Landscape

As a cybersecurity company headquartered in Singapore and operating across multiple jurisdictions, Group-IB is subject to a layered set of obligations. We distinguish three: sustainability-reporting regulation; the voluntary frameworks we apply; and the operational, data-protection, and sector regulation that governs how we run the business.

On sustainability-reporting regulation, we have assessed our position under the EU Corporate Sustainability Reporting Directive (CSRD), as amended by the Omnibus I Directive (Directive (EU) 2026/470). Under the revised rules, a non-EU parent falls within scope only where it generates net turnover in the EU above EUR 450 million for two consecutive years and maintains an EU subsidiary or branch exceeding EUR 200 million in net turnover; for in-scope non-EU groups, first reporting applies to the 2028 financial year. On the basis of current turnover, Group-IB does not meet these thresholds and is therefore not within the mandatory scope of the CSRD — to be confirmed against audited financial figures. In parallel, we monitor developments in our headquarters jurisdiction, where Singapore is phasing in climate-related disclosure requirements aligned with the ISSB Standards, and we treat this Report as part of our readiness for any future mandatory obligation.

Domain	Framework / Regulation	Jurisdiction(s)	Group-IB Status
Sustainability reporting	GHG Protocol (Corporate Standard)	Global	Applied
Sustainability reporting	GRI Standards	Global	Proposed primary framework
Sustainability reporting	ISSB (IFRS S1 / S2); TCFD	Global / Singapore	Referenced for climate
Sustainability reporting	EU CSRD (Directive (EU) 2026/470)	European Union	Monitored — not currently in scope
Data protection	EU GDPR	European Union	Compliant
Data protection	PDPA	Singapore	Compliant
Data protection	PDPL and regional data-protection laws	UAE, KSA, others	Compliant
Operational resilience	DORA	European Union	Addressed for EU clients
Operational resilience	NIS-2 Directive	European Union	Addressed for EU clients
AI governance	EU AI Act	European Union	Alignment planned (2026)
AI governance	NIST AI RMF; ISO/IEC 23894:2023	Global	Applied (Responsible AI)
Information security	ISO/IEC 27001:2022 (TÜV Austria)	Global	Certified
Quality management	ISO 9001:2015 (TÜV Austria)	Global	Certified
Security assurance	SOC 2 Type II	Global	Planned for 2027-2028
National security framework	Applus+ ENS-High	Spain	Certified
Integrity / law enforcement	US DoJ compliance (Deloitte attestation)	United States	Attested
Managed security services	Managed SOC and Monitoring Service License	Singapore	Licensed

01

Group-IB at a Glance

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

About Group-IB

Founded in 2003, Group-IB is a creator of predictive cybersecurity technologies established to investigate, prevent and fight digital crime. Headquartered in Singapore, and with Digital Crime Resistance Centers in Latin America, Europe, META, Central Asia, and the Asia-Pacific, Group-IB delivers predictive, intelligence-driven defense by analyzing and neutralizing regional and country-specific cyber threats via its Unified Risk Platform, offering unparalleled defense through its industry-leading Cyber Fraud Intelligence Platform, Cloud Security Posture Management, Threat Intelligence, Fraud Protection, Digital Risk Protection, Managed Extended Detection and Response (XDR), Business Email Protection, and External Attack Surface Management solutions, catering to government, retail, healthcare, gaming, financial sectors, and beyond. Group-IB collaborates with international law enforcement agencies like INTERPOL, Europol, and AFRIPOL to fortify cybersecurity worldwide, and has been awarded by advisory agencies including Gartner, Forrester, Datos Insights, Frost & Sullivan, and KuppingerCole.

Mission

Group-IB's corporate mission is **"To Fight Against Cybercrime"**, by developing advanced cybersecurity technologies to investigate, predict, prevent, and fight digital crime, strengthening global digital safety and trust.

We exist to protect organizations, individuals, and society from acts of injustice, intervening where criminal activity threatens business operations, financial integrity, public confidence, or national and regional security. This translates into actionable intelligence, faster threat mitigation, and resilient protection for our stakeholders against cyber and fraud risks that could otherwise undermine growth, reputation, and trust.

Vision

To combat the rapid advancement of cybercrime, several critical elements are required:

1. Comprehensive, cross-regional threat visibility, enabled by predictive threat intelligence and cyber-fraud fusion that exposes end-to-end malicious infrastructure.
2. The ability to disrupt cybercriminal infrastructure in real-time, regardless of geographic or jurisdictional boundaries.
3. Predictive defense capabilities that anticipate future attacks and dynamically adjust protection as threats evolve.

To deliver this at scale, our goal is to develop a "glocal" company, one that is global in reach, yet locally embedded. This enables us to deliver bespoke solutions, services and unique context-aware insights tailored to the local cyber environments and threat landscapes our clients operate in.

This strategic shift deepens our engagement with regional communities, while playing a crucial role in strengthening national cybersecurity postures.

By establishing local Digital Crime Resistance Centers, we can better understand and address specific threats faced by each country or region, enabling Group-IB to develop targeted, intelligence-led solutions that align with national security priorities, helping organizations reduce risk faster, respond more effectively, and protect what matters most.

Principles

Zero tolerance for cybercrime
We fight cybercrime in all its forms, regardless of geography, background, or target. Our decisions are driven by evidence, not external pressure. Our international team, clients, and research partners help us maintain independence and neutrality in everything we do.

We reduce cybercrime worldwide
We take responsibility for protecting people, businesses, and countries worldwide. Through our products, services, threat research, and cooperation with international law enforcement, we work to reduce the number of active criminal organizations and make the digital world safer.

Our success is not measured by money
We generate profit to fight cybercrime effectively, not the other way around. We share our expertise with companies, NGOs, and public institutions beyond our commercial clients because our success is measured by the cybercriminals we stop, not the profit we make.

We investigate and analyze
Our teams investigate how cybercrime operates and share intelligence with clients, partners, regulators, law enforcement, and the cybersecurity community. Through research, public reports, and our Academic Alliance, we combine expertise across disciplines to better understand and counter evolving threats.

We invent and improve
We don't follow well-trodden paths. With 150 patents and patent applications and innovations like BioConfirm, the Cyber Fraud Intelligence Platform, and Next-Gen Fraud Matrix 2.0, we continuously invest in proprietary R&D to stay ahead of evolving cybercrime.

Progress in 2025

In 2025, we expanded our operational footprint to **11 Digital Crime Resistance Centers (DCRC)** with locations in Singapore, the Netherlands, the United Arab Emirates, Chile, Saudi Arabia, Egypt, Thailand, Malaysia, Vietnam, Italy and Uzbekistan. Two flagship facilities were launched during the year: **the Singapore Cyber Fusion Center,** the first Cyber Fusion Center in the Asia-Pacific region, and **the Cairo DCRC,** inaugurated in May 2025 to deepen the company's role across North Africa.

From these regional hubs, a workforce of **556 employees** representing more than **30 nationalities** serves a customer base of **450+ organizations** in over **60 countries** and in more than **20 languages,** across financial services, government, telecommunications, e-commerce, and critical infrastructure.

Our business model is grounded in proprietary technology developed and protected through a portfolio of **150 patents** and patent applications. In 2025, Group-IB filed its first patent in Saudi Arabia, expanding the portfolio's geographic reach, and continued active filings in the United States, the Netherlands, and Singapore.

The company's core Unified Risk Platform brings together **Threat Intelligence, Fraud Protection, Managed XDR, Digital Risk Protection, Attack Surface Management, and Business Email Protection,** complemented in 2025 by new offerings including BioConfirm biometric authentication, **the Cyber Fraud Intelligence Platform** (validated by Bureau Veritas as GDPR-compliant), **the Next-Gen Fraud Matrix 2.0 framework,** and **an LLM-powered AI Assistant** (beta, launched April 2025) embedded in the Threat Intelligence platform. These solutions are reinforced by Group-IB's proactive and reactive services — **Digital Forensics** and **Incident Response** (named among the Representative Vendors in Gartner's Market Guide for DFIR Retainer Services), **Audit and Consulting, Hi-Tech Crime Investigations, and Education and Training** delivered through Group-IB Academy — together representing more than **1,540 successful high-tech crime investigations** to date.

Group-IB's impact extends beyond commercial cybersecurity. In 2025, the company's investigative support contributed to **six international operations** coordinated with INTERPOL, Europol, AFRIPOL, and 52 national law enforcement agencies, resulting in the arrest of **1,809 cybercriminals** and the takedown of more than **34,838 pieces of malicious infrastructure.**

Our operations are overseen by a Code of Conduct refreshed in 2025, with **100% compliance** reported across all employees, contractors, customers, suppliers, and partners, and underpinned by ISO 9001 and ISO 27001 certifications, a Deloitte attestation of compliance with US Department of Justice requirements, Singapore Penetration Testing License and Applus+ ENS Certification in Spain.

Together, global scale, proprietary innovation, and structured collaboration with the public sector define Group-IB's role in the cybersecurity value chain — a technology company whose core business is, by design, a contribution to a safer digital ecosystem.

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

2003
Year Founded

450+
Customers

1,809
Cybercriminals Arrested Across Six Operations

2025 INTERPOL-Linked Outcomes. Secure, Serengeti 2.0, Red Card, Big Bang, Contender 3.0 and ALTDOS

34,838
Pieces of malicious infrastructure dismantled

2025 Law Enforcement Collaboration Outcomes

11
Digital Crime Resistance Centers

Including the new Singapore Cyber Fusion Center and the new Cairo DCRC

150
Patents and Patent Applications

First patent filing in Saudi Arabia in 2025, expanding geography; active filings continued in the United States, the Netherlands, and Singapore

1st
Private company to offer cybercrime investigation services

Market Position

58%
Year-on-year increase in advanced persistent threat (APT) activity

Documented in the High-Tech Crime Trends Report 2026

1,540+
Successful high-tech crime investigations

Investigations to Date

60+

Countries Served

15+
University partnerships across 11 countries. 400+ students engaged

Academic Alliance

Gartner's Market Guide
Named among the Representative Vendors in Gartner's Market Guide for DFIR Retainer Services

Market Position

556

Employees

30+

Nationalities Represented

20+
Languages, one seamless service experience

Operational Footprint

Singapore
Group-IB Global Private Limited

HQ Location

ISO 9001 and ISO 27001
Quality Management and Information Security

Certifications

DOJ-Compliant
Deloitte attestation of compliance with US Department of Justice requirements

Certifications

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Products and Services

The Unified Risk Platform

Group-IB delivers cybersecurity through a single, intelligence-driven architecture — the Unified Risk Platform — that maps each client's threat profile, correlates signals across attack surfaces, and tailors defensive action in real time. At its core is the Unified Intelligence Engine, which combines an Intelligence Data Lake of signals, telemetry, intelligence, and context with AI-driven reasoning, analysis, orchestration, and prediction. The engine is fed by Group-IB's human and machine intelligence producers: Incident Response, Hi-Tech Crime Investigations, CERT, threat researchers, fraud analysts, and detection and intelligence systems.

In 2025, the portfolio product line expanded into adjacent threat domains, with new platform modules, two new product launches, and a strengthened services layer.

Across every solution, Group-IB's sustainability value proposition is the same: cybersecurity is digital infrastructure that protects business continuity, revenue integrity, and customer trust — and, by neutralizing botnets, fraud rings, and ransomware operations, delivers measurable environmental and societal externalities.

Product Lines

The Unified Risk Platform is organized into four product lines.

1. Cyber Intelligence: gives organizations visibility into threats and exposures beyond their perimeter. It comprises Threat Intelligence, which delivers the proprietary data, malware analysis, and threat-actor profiling that underpin proactive defense; Digital Risk Protection, which secures brand and digital assets; Attack Surface Management continuously discovers and monitors external IT exposure; and Cloud Security Posture Management, added in 2025 to extend coverage into multi-cloud risk. In April 2025 Threat Intelligence was augmented by an LLM-powered AI Assistant that lets analysts query Group-IB's threat data in natural language and conducts automated research. The agentic successor was released as Prevyn AI in May 2026, following the close of the reporting period.
2. Managed XDR provides round-the-clock detection and response across endpoints, networks, infrastructure, and email. It brings together Endpoint Detection & Response, Network Traffic Analysis, the Malware Detonation Platform, and Business Email Protection, which blocks and hunts advanced email threats.
3. Fraud Prevention safeguards digital revenue across banking, fintech, e-commerce, and gaming. It comprises Fraud Protection,



01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

BioConfirm Authentication, Fraud Intelligence, and the Cyber Fraud Intelligence Platform. **BioConfirm,** launched in July 2025, is a real-time biometric authentication solution that combines face and fingerprint with cryptographic tokens to defend against deepfakes, SIM-swap, and emulators in PSD2, RBI, and CBUAE environments.

4. Services extend the platform with **expert-led capabilities:** Investigation and Incident Response, Assessments and Consulting, and Training and Education.

New Platform-Grade Launches in 2025

Two new platform-grade launches expanded the boundary of what Group-IB delivers:

- **The Cyber Fraud Intelligence Platform (CFIP),** introduced in December 2025, is positioned as the first GDPR-compliant collective anti-fraud intelligence platform, built on a patented Distributed Tokenization architecture that enables banks, telecoms, e-commerce, and gaming companies to exchange real-time risk signals without exchanging personal data; the platform was independently validated by Bureau Veritas.
- **The Next-Gen Fraud Matrix 2.0,** released in July 2025, is a public taxonomy of fraud tactics and techniques modeled on MITRE ATT&CK, extending classification to cross-industry procedures and supporting standardization across the anti-fraud ecosystem.

Services and Knowledge Layer

These technologies are complemented by a structured services layer — **Digital Forensics and Incident Response (DFIR), Audit and Consulting, and Hi-Tech Crime Investigations** — together representing more than **1,540 successful high-tech investigations** conducted to date and **77,000+ hours of incident response** delivered by the DFIR Lab in 2025.

2025 Recognition

Recognition for Group-IB in 2025 came from various stakeholder groups. Together, the awards, certifications, and partnerships formalized in 2025 validate three strategic shifts the company is making: from technology vendor to ecosystem orchestrator, from regional cybersecurity firm to global Tier-1 platform provider, and from commercial security supplier to recognized contributor to the public-interest digital safety agenda.

1. Technological Innovation
   - **KuppingerCole —** Overall Leader, Fraud Reduction Intelligence Platforms. Independent positioning at the top tier of the fraud-prevention category validates the maturity of Fraud Protection and the early traction of CFIP and BioConfirm against established competitors.
   - **Frost & Sullivan** — Technology Innovation Leadership. Confirms that Group-IB's investment in proprietary R&D is translating into recognized technical differentiation rather than incremental feature parity.
   - **Gartner** — Market Guide for Digital Forensics and Incident Response Retainer Services. Named among the Representative Vendors in Gartner's Market Guide for DFIR Retainer Services — providers for which Gartner received the highest levels of client interest. The listing reflects the market credibility of Group-IB's Services Retainer, which combines incident response with threat intelligence, forensics, malware analysis, and threat hunting across 60+ countries.
   - **Responsible disclosure:** CVE-2025-20374 (Cisco UCCX) and CVE-2025-36135 (IBM Sterling). Two zero-day vulnerabilities discovered by Group-IB's Red Team and disclosed responsibly to global vendors. Both were patched, demonstrating direct, measurable contribution to the security of widely deployed enterprise infrastructure.
   - **MITRE ATT&CK v17** — two techniques contributed by the APAC team. T1564/013 (Bind Mounts) and T1564/014 (Extended Attributes) added to the global open standard for attack classification. A non-commercial, infrastructure-level contribution to the cybersecurity commons.
   - **High-Tech Crime Trends 2026** — Forbes, VTM, global Tier-1 media coverage. Flagship public research, based on 1,540+ investigations and reporting a 58% YoY rise in APT activity, anchored Group-IB's thought-leadership position across four regional editions in 2025.
2. Sustainability and Public-Interest Leadership
   - **ESG thought leadership:** The Business Times (Singapore) and Forbes Middle East. Connecting cybersecurity to climate and sustainability outcomes — externally validating Group-IB's position that cybersecurity is a sustainability discipline.
   - **INTERPOL, Europol, AFRIPOL, and 52 national law enforcement agencies** — six joint operations. Operations against ALTDOS, Operation Secure, Serengeti 2.0, Red Card, Big Bang, and Contender 3.0 produced **1,809 arrests, $97.4M recovered** (Serengeti 2.0 alone), and **34,838 takedowns** of malicious infrastructure — quantifying Group-IB's contribution to global digital safety.
   - **Botswana (BOCRA) and Kyrgyzstan (Ukuk)** — national-cyber-defense MoUs. Government-to-company partnerships formalize Group-IB's role as a long-term capability-building partner in emerging cybersecurity markets, beyond commercial sale.
3. Certifications and Compliance Assurance
   - **ISO/IEC 27001:2022 (TÜV AUSTRIA).** Independent attestation that Group-IB's information security management system meets the most recent global standard — operationally relevant given the company processes high-sensitivity threat data on behalf of clients.
   - **ISO 9001** — Quality Management Systems. Demonstrates that delivery processes across investigations, MXDR, and platform operations are governed by an audited quality framework.
   - **Deloitte attestation** — compliance with US Department of Justice requirements. Validates Group-IB's operational integrity at a level required for engagement with US public-sector and regulated industry clients.
   - **Singapore** — Managed Security Operations Center and Monitoring Service License. Confirms regulatory standing in Group-IB's headquarters jurisdiction and underpins the credibility of the new Singapore Cyber Fusion Center.
   - **Bureau Veritas** — independent validation of the Cyber Fraud Intelligence Platform. Third-party verification of CFIP's GDPR-compliant Distributed Tokenization architecture confirms that collective anti-fraud intelligence can be exchanged across institutions without compromising personal data — a privacy-by-design milestone for the sector.
   - **Applus+ ENS Certification** — High — National Spanish Certification for the highest compliance standards in cybersecurity solutions.
4. Industry and international
   - **WEF Cybercrime Atlas (January 2025).** Group-IB analysts contributing to Cybercrime Mapping and Investigation Working Groups embed the company in the world's most senior cross-sector cybercrime coordination platform.
   - **MITRE Fight Fraud Framework (F3) (April 2025).** Co-developing the cross-industry fraud taxonomy positions Group-IB as a standards-setting participant, complementing the public release of Next-Gen Fraud Matrix 2.0.
5. Commercial and channel
   - **European Partner Program with Group-IB Partner Academy (April 2025).** Free, structured certification for European partners. Anchors the company's 5-Star CRN Partner Program Guide 2025 rating.
   - **MoUs at GISEC Global 2025 (May 2025).** Regional partnerships across META that scale market access beyond direct sales.
   - **Neverhack (September 2025), Cyber Samurai / DACH (September 2025), SecurityHQ** — global MSSP partnership, VAS Integrated Solutions / KSA (December 2025). Strategic channel and MSSP expansions extending Group-IB's reach into Europe, DACH, and Saudi Arabia through operationally embedded partners.
   - **UAE Cybersecurity Council** — Outstanding Partner (GISEC). Government-level recognition in one of Group-IB's most strategic regional markets.
   - **Singapore Police Force** — recognition for outstanding contribution to tackling cybercrime. Public-sector acknowledgment in Group-IB's headquarters jurisdiction, supporting the credibility of the Singapore Cyber Fusion Center.

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

6. Academic Alliances
- Cyber University Tashkent (October 2025)
- NP Ngee Ann Polytechnic (Singapore)
- Nebrija University (Spain)
- LISA Institute (Spain)
- National Polytechnic University of Armenia
- CSU University (Uzbekistan)
- TACTIC Academy with KPMG Italy
- Serbia National CERT (June 2025)

Academic Alliance grew to **15+ partnerships** across **11 countries** with **40+ certified professors annually.** Directly supports the 1,000 STEM specialists by 2027 social commitment and the 400+ students who passed through Group-IB academic programs in 2025.

7. Workplace and Social Excellence
- Top Women in Security ASEAN 2025. Continued recognition of female leadership at Group-IB (Jessica Tedja, Singapore winner) reinforces inclusion in a sector where female representation remains structurally low.
- Inc. Arabia — Cybersecurity Leader of Tomorrow. Regional recognition that validates the next generation of leadership emerging from Group-IB's META operations.
- CRN Partner Program Guide 2025 — 5-Star Rating. Independent assessment of partner training and certification programs by CRN underscores the strength of the Partner Academy and the company's commitment to ecosystem capability-building.

02 Cybersecurity

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Group-IB delivers cybersecurity protection across the global digital ecosystem in pursuit of its founding mission to fight against cybercrime. Continuous cyber defense, frontier research, international coordination, and capacity building — these dimensions of the company's work are the operational expression of that mission and essential contribution to our E, S and G efforts.

Our flagship public research, **the High-Tech Crime Trends Report 2026**, drawing on **1,540+ Group-IB investigations**, documented a disturbing **58% year-on-year increase in advanced persistent threat (APT)** activity. The analytical focus of the research shifted decisively toward the structural fragility of **digital supply chains**, which collectively affected tens of millions of end users, dozens of financial institutions and enterprises, and produced direct losses measured in billions of dollars. We have also highlighted our participation in **six international cybercrime prevention operations** across four regions performed in collaboration with both global and national law enforcement agencies.

Group-IB's **Computer Emergency Response Team (CERT-GIB)** operates round the clock, delivering continuous protection to commercial customers and public sector institutions across key areas of the company's presence.

Active accredited membership in the principal international response networks such as FIRST, the Trusted Introducer, APCERT, OIC-CERT, and APWG, together with structured participation in the World Economic Forum's Cybercrime Atlas and INTERPOL, secures our status as a trusted partner to the key institutions shaping global cybersecurity policy.

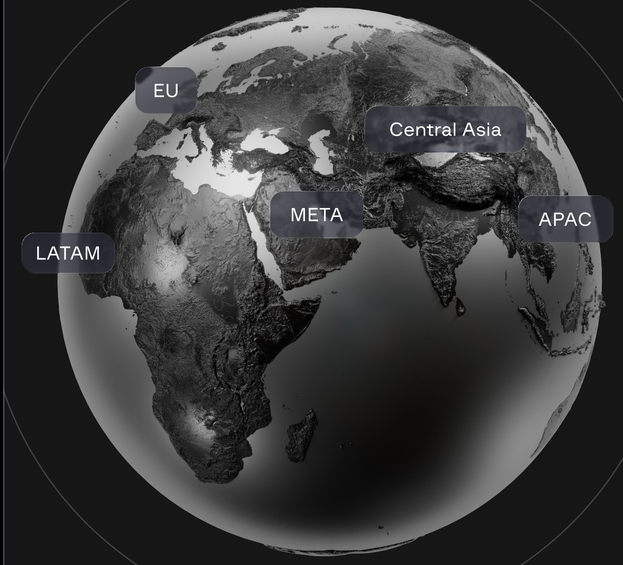
Research and development continued to translate into tangible product advantage, built on a portfolio of **150 patents** and patent applications and expressed in new offerings such as BioConfirm biometric authentication, the Cyber Fraud Intelligence Platform (validated by Bureau Veritas as GDPR-compliant), the Next-Gen Fraud Matrix 2.0 taxonomy, and an LLM-powered AI Assistant (beta, launched April 2025) embedded in the Threat Intelligence platform.

As **artificial intelligence** moves from supporting tool to core capability, we acknowledge that public statements of intent must be supported by formal legal grounds for responsible AI use. As a first step, we built an internal **Responsible AI Policy** and achieved 100% penetration across the company. With an increasing importance of AI we will continue to formalize the principles of AI implementation throughout our products and services portfolio.

Across both product innovation and AI deployment, **data privacy** assurance is anchored by ISO/IEC 27001:2022 certification (TÜV Austria), GDPR-aligned controls, and independent Bureau Veritas validation of the Cyber Fraud Intelligence Platform's privacy-by-design Distributed Tokenization architecture.

Cybersecurity education and capacity-building are central to how we transfer knowledge openly to industry professionals, regulators, and the next generation of specialists. In 2025, we extended free specialized training to channel our partners in Europe through the **Partner Academy.** Through the Academic Alliance, now spanning **15+ university** partnerships across **11 countries**, more than **400 students** engaged with Group-IB academic programs.

Law Enforcement Operations per Region in 2025



19,950

~55 per day

Blocked phishing hosts

287,425

~790 per day

Blocked scam hosts

558 mln

Hi-scored fraud sessions (FP)

~860,000 people per day

314 mln

Identities protected from fraud (FP)

~1 060 per minute

708 mln

Devices protected from fraud (FP)

~1.9 mln devices per day

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

High-Tech Crime Trends Report 2026

Group-IB's flagship public research — the High-Tech Crime Trends Report 2026 (HTCT) — was disseminated during the year through four regional editions covering META, Asia-Pacific, LATAM, and Europe, with a Global edition published in March 2026. Drawing on the analysis of more than **1,540 Group-IB investigations**, the Report documented a **58% year-on-year increase in advanced persistent threat (APT)** activity and quantified the company's contribution to law-enforcement-led mitigation across 2025.

52
National law enforcement agencies supported

6
Global operations conducted with Group-IB participation

1,809
Cybercriminals arrested with Group-IB's contribution

310,643
Victims of cybercriminal activity confirmed

34,838
Pieces of malicious infrastructure and resources dismantled

>USD 100 million
In estimated cybercriminal financial damage averted across Group-IB-supported operations

>1,540
Successful investigations conducted by the Group-IB High-Tech Crime Investigations Department

>77,000 hours
Of incident response delivered by the Group-IB Digital Forensics and Incident Response (DFIR) Lab

The Report's analytical center of gravity shifted decisively toward the structural vulnerability of **digital supply chains.** By compromising upstream vendors, SaaS platforms, open-source projects, and managed service providers, attackers in 2025 inherited trusted access to hundreds of downstream organizations — transforming single intrusions into cascading, multi-victim incidents. As the Report concludes, trust is no longer implicit; it must be verified, monitored, and secured continuously. This pattern was visible across the year's most consequential breaches, which collectively affected many millions of end users, hundreds of enterprises including dozens of financial institutions, and produced direct losses measured in billions of dollars.

Reference supply-chain incidents

Oracle
6 million users; 128,465 domains compromised via exploitation of a legacy environment

Salesloft • Drift • Salesforce
700+ organizations impacted through compromised OAuth tokens across an interconnected SaaS chain

Marquis
74 banks affected; up to 1.35 million individuals exposed via a ransomware attack on a fintech vendor

Shai-Hulud
180 to 800 npm packages compromised via a self-propagating worm in the open-source supply chain

Jaguar Land Rover (JLR)
GBP 196 million in operational damage

Cyberhaven
2.6 million users exposed

Bybit
USD 1.5 billion

Trust Wallet
USD 8.5 million

Cooperating for Digital Security

Group-IB's direct contribution to digital trust came through structured collaboration with **INTERPOL, Europol, AFRIPOL, and 52 national law enforcement agencies.** This partner posture translated into six coordinated international operations during the year — the joint action against **ALTDOS, Operation Secure, Operation Red Card, Operation Serengeti 2.0, Operation Big Bang, and Operation Contender 3.0** — which together produced **1,809 arrests** of cybercriminals and contributed to the takedown of **34,838 pieces** of malicious infrastructure across Group-IB's wider mitigation activity.

Asia-Pacific

Operation Secure February 2025
Produced 32 arrests, the seizure of 41 servers, and the disruption of more than 20,000 malicious IPs and domains, with Group-IB's technical support coordinated through INTERPOL's Cybercrime Directorate. The Singapore Police Force separately recognized Group-IB in 2025 for outstanding contribution to tackling cybercrime in Singapore, extending the partnership noted in the 2024 Report

META

Operations Red Card April 2025
Contender 3.0 October 2025
Contributed a further 566 arrests across the region — 306 and 260 respectively — with Contender 3.0 also resulting in the seizure of 1,235 devices and the identification of 1,463 victims

Operation Serengeti 2.0 August 2025
Produced 1,209 arrests, the disruption of 11,432 criminal networks, the return of USD 97.4 million to victims, and the protection of approximately 88,000 individuals

Europe

Operation Big Bang September 2025
Culminated in the arrest of the threat actor known as "GoogleXCoder" and the dismantling of more than 250 phishing sites targeting European consumers

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Latin America

Group-IB extended its Digital Crime Resistance Center presence in Chile and provided incident-response support to national institutions through Group-IB Consultoria LATAM, with operational detail subject to confidentiality undertakings

Infrastructure Resilience and Data Privacy

The Cyber Fraud Intelligence Platform (CFIP), launched in December 2025, is positioned as direct infrastructure-layer mitigation, enabling cross-institutional risk-signal exchange under a GDPR-compliant, privacy-by-design architecture independently validated by Bureau Veritas.

Continuous Research and AI

Group-IB's research and development output reflects a deliberate balance between operating at the technical frontier of threat intelligence and applying artificial intelligence responsibly. These efforts translated into a tangible product advantage, built on a portfolio of 150 patents and patent applications and expressed in new offerings such as BioConfirm biometric authentication, the Cyber Fraud Intelligence Platform (validated by Bureau Veritas as GDPR-compliant), the Next-Gen Fraud Matrix 2.0 taxonomy, and an LLM-powered AI Assistant (beta, launched April 2025) embedded in the Threat Intelligence platform.

We advanced a public Responsible AI position through the AI Cybersecurity Hub, articulating Explainable AI, human-in-the-loop deployment, and alignment with the NIST AI Risk Management Framework, ISO/IEC 23894:2023, and the EU AI Act, with a formal Responsible AI Policy on track for publication in 2026.

The Red Team's discovery and disclosure of two zero-day vulnerabilities — CVE-2025-20374 in Cisco Unified Contact Center Express and CVE-2025-36135 in IBM Sterling — was confirmed and patched by the vendors in December 2025, contributing directly to the security of widely deployed enterprise infrastructure used by millions of end customers. Two new techniques were accepted into MITRE ATT&CK v17, the global open standard for attack classification used by thousands of organizations worldwide.

Responsible Disclosure

CVE-2025-20374

Cisco Unified Contact Center Express — discovered by Group-IB Red Team, responsibly disclosed, confirmed and patched by Cisco (December 2025)

CVE-2025-36135

IBM Sterling — discovered by Group-IB Red Team, responsibly disclosed, confirmed and patched by IBM (December 2025)

Open-standards contribution

MITRE ATT&CK v17 (2025)

T1564/013 "Bind Mounts" (Nam Le, APAC)
T1564/014 "Extended Attributes" (Sharmine Low, APAC)

Partnership for Cybersecurity

Developing cross-industry partnerships, continuous training and open transfer of cybersecurity knowledge are essential to Group-IB. We continued to build a shared cybersecurity knowledge base and to transfer it openly to industry professionals, regulators, and the next generation of specialists.

In 2025, we delivered 55 customer-facing training sessions and provided free specialized training to channel partners in Europe through The Partner Academy launched in April 2025 and recognized with a 5-Star Rating in the CRN 2025 Partner Program Guide.

The Academic Alliance now spans across 15+ university partnerships in 11 countries, with more than 40 certified professors annually teaching in four languages and engaging 400+ students through the student-operated Security Operations Center (SOC), the Threat Intelligence Academy, Capture the Flag competitions, and internships, advancing the company's commitment to support 1,000 future STEM specialists by 2027.

Public threat-research output, including more than 46 technical blogs and threat research reports, achieved institutional uptake during the year through citation by the FBI and the American Bankers Association in their joint Deepfake Voice Phishing advisory and through use by regulators and journalists in more than ten countries.

Client and Partner Training

Customer-facing technical training

55 sessions delivered in 2025
918 hours of structured education

Group-IB Academy

873 course completions
Approximately 1,300 additional learning hours

Partner Academy

Free specialized training for channel partners in Europe
Recognized with a 5-Star Rating in the CRN 2025 Partner Program Guide

Academic Capacity-building

Academic Alliance footprint

15+ university partnerships across 11 countries;
40+ certified professors annually; instruction in four languages

Students reached

400+ students in 2025 through student-operated SOC, Threat Intelligence Academy, CTF competitions, and internships

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

40+

Professors Certified
Train-the-Trainer Program — our flagship approach

Key Projects

Hands-on student access to our Threat Intelligence and MXDR platforms, Train-the-Trainer enablement, and Student SOC labs — building practical, real-world cybersecurity skills

Global Event Participation

Engaging students worldwide through flagship cybersecurity events — including ICO 2026 — building visibility and the next generation of defenders

International Cybersecurity Olympiad (ICO) 2026

Key Numbers

11
Countries reached

400+
Students Taught

4
Regions: APAC, META, Central Asia, Europe

12
Active projects at universities

New Academic Partnerships 2025

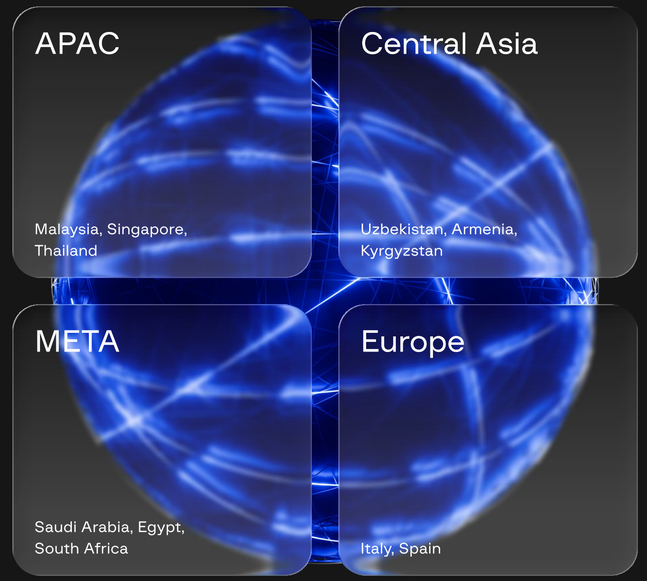
Coventry University, Egypt

Universidad Nebrija, Spain

Armenia National Polytechnic University, Armenia

LISA Institute, Spain

Academic Alliances Global Presence



03

ESG Strategy

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

ESG at Group-IB

Group-IB's Environmental, Social, and Governance commitment aligns with the company's mission to fight cybercrime and is therefore naturally intertwined with its operations. Our second Sustainability Report reaffirms our commitment to the goals set earlier and openly shares our progress on them.

In 2025, we successfully progressed toward our social targets by providing sustainability training for our workforce, which explained the basic principles of the Environment, Social, and Governance pillars at Group-IB, as well as the company's broader sustainability efforts.

Although we have not set any environmental targets to lower emissions against our 2024 baseline year, we have continued our voluntary efforts to measure our carbon emissions in alignment with the globally acknowledged Greenhouse Gas (GHG) Protocol standard and optimize, where possible, our resource usage in the regions of our presence. An example of this effort is our European office, which continues to power its operations using local renewable energy sources.

Supported by our professional workforce, which has grown by 25% since 2024 and now totals 556 employees, we were able to support operations in 60 countries through our 11 offices. We continued educating professionals by providing specialized training and fostering our academic partnerships, which now include 15+ universities in 11 countries. Additionally, we launched the Group-IB Partner Academy and expanded our online educational and research resources with webinars, podcasts, and the new issue of our flagship High-Tech Crime Trends Report 2026.

Advancing our governance-related targets, we shared our updated policies, such as the Code of Conduct and Privacy Policy, with 100% of employees successfully completing corporate training on their implementation. We are also further extending these policies to our suppliers.

Our Sustainability Targets Progress

Social

- Provide internal training programs focused on ethics and sustainability to >90% employees.
  Deadline: 2026.
  Status: 100% complete.
  100% employee participation in Code of Conduct and company's sustainability efforts training.
- Support the development of 1,000 future Science, Technology, Engineering, and Mathematics (STEM) professionals by investing in cybersecurity education programs, partnerships with schools and universities, and inclusive mentorship initiatives.
  Deadline: 2027.
  Status: 35% of target complete with 2 years remaining.
  400+ students have been educated via company's educational programs through academic partnerships.

Governance

- Develop and publish an ESG program and materiality matrix.
  Deadline: 2026.
  Status: in progress.
  ESG program and materiality matrix are being developed subject to publication in 2027.
- Embed ESG principles into procurement through a supplier Code of Conduct and Due Diligence Framework, screen 100% of suppliers.
  Deadline: 2026.
  Status: 100% complete.
  Updated Code of Conduct has been published in the Sustainability section on the website. 100% of suppliers are monitored using the new Due Diligence Framework.

ESG Leadership

Leadership and accountability for ESG at Group-IB rests with the Deputy CEO, Anastasiia Komissarova, who sets the direction of the company's sustainability disclosures and chairs a cross-departmental ESG Working Group. The Working Group draws on senior representatives from Legal and Compliance, HR, Security, Product, PR, Marketing, and Finance, and reports into the Board of Directors. The Board reviews progress quarterly against the indicators disclosed in this Report, including progress against each ESG target, climate-related risks and opportunities, and stakeholder-engagement outcomes.

The Board's sustainability oversight is supported by regular ESG and climate-risk briefings delivered by external experts and by annual evaluations that assess ESG integration, stakeholder engagement, and risk-management effectiveness. A direct escalation channel allows any senior manager to raise critical ESG, compliance, or ethical concerns to the Board outside the scheduled review cycle.

Day-to-day management of ESG is led by the company's ESG Manager, who reports to the Deputy CEO. The ESG Manager coordinates delivery against the company's ESG targets, owns the preparation of this Report and the company's ongoing sustainability disclosure, and promotes ESG initiatives across the organization — translating the strategy set by the Working Group into measurable progress.

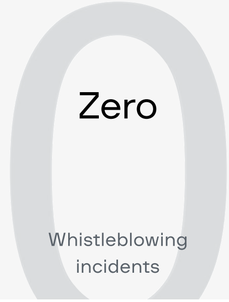
Our ESG Data 2025



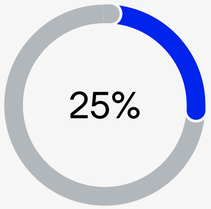
Code of Conduct ↗
compliance



Privacy Policy ↗
compliance



Whistleblowing incidents



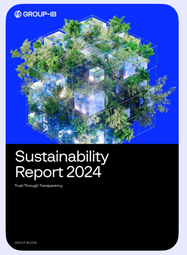
Increase in workforce year-on-year

>1,540

Successful investigations conducted by the Group-IB High-Tech Crime Investigations Department

>77,000 hours

Of incident response delivered by the Group-IB Digital Forensics and Incident Response Lab



Sustainability Report 2024 ↗

This report covers the sustainability-related strategy, policies, and performance of Group-IB Global Private Limited and its subsidiaries across key operational regions.

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

ESG Leadership Structure

Board of Directors
Oversight of ESG strategy and material sustainability risks; quarterly review of progress against each ESG target, climate-related risks and opportunities, and stakeholder-engagement outcomes; supported by ESG and climate-risk briefings and an annual ESG-integrated evaluation.

Executive accountability
Anastasiia Komissarova, Deputy CEO; sets the direction of ESG disclosure and chairs the cross-departmental ESG Working Group.

Cross-department ESG Working Group
Senior representatives from Legal and Compliance, HR, Security, Product, PR, Marketing, and Finance; reports into the Board of Directors.

ESG Manager
Coordinates ESG delivery and disclosure; supports the Working Group and reports to the Deputy CEO.

> Every supplier now goes through our Due Diligence Framework before we work with them, and our Code of Conduct training reaches 100% of employees rather than a subset. What I'm proudest of is the escalation channel we built so any senior manager can raise a concern directly with the Board, outside the normal review cycle. Governance only means something if people can act on it when it matters, not just report on it once a quarter.



Anastasiia Komissarova
Deputy CEO

Material Topics

Group-IB's materiality assessment identifies the **environmental, social, governance,** and **digital security and AI** issues most likely to affect our business resilience and stakeholders. Each topic is evaluated for its significance to our long-term performance and its relevance to the stakeholders we serve.

This year's assessment formalizes **digital security and AI** as a distinct fourth pillar, reflecting its centrality to Group-IB's mission. As a cybersecurity company, our most significant impacts are not only operational but also reputational and societal: the integrity of the systems we protect, the technologies we deploy, and the expertise we build and share across the industry.



Footprint of operations
Energy consumption and greenhouse gas emissions from offices and the data infrastructure underpinning our threat-intelligence and detection platforms, where compute-intensive workloads are the primary driver of energy demand.



People, ethics, and culture
Safe, equitable working conditions, talent retention, and conduct standards across a geographically distributed, highly specialized technical workforce.

Cybersecurity workforce development
Recruiting, training, and retaining cybersecurity professionals to address the global skills shortage that constrains both our operations and the wider industry.

Community impact through capacity-building
Strengthening the broader security ecosystem through training, knowledge transfer, and support for under-resourced institutions.



Economic performance and business conduct
Financial sustainability and ethical commercial practice across the markets in which we operate.

Anti-corruption, compliance, and certifications
Adherence to anti-corruption controls, regulatory obligations, and internationally recognized certifications, that govern how we operate.

Data privacy and digital rights
Lawful, proportionate handling of the sensitive threat, incident, and personal data we process during investigations and threat intelligence work, and respect for digital rights in how that data is collected and used.

Supply-chain integrity
Security and resilience of our vendor and technology supply chain, where third-party compromise is a direct risk to the assurances we provide clients.



Responsible AI governance
Controls ensuring AI systems used in detection and response are deployed accurately, transparently, and without unintended harm.

Development and deployment of new technologies
Disciplined adoption of emerging technologies to keep pace with evolving threats while managing associated risks.

Knowledge sharing
Open disclosure, including through this Report, on the global state of cybercrime to inform clients, partners, and the public.

Educating cybersecurity professionals
Building industry-wide capability through structured training and the transfer of specialized expertise.

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

ESG Risks and Opportunities

Group-IB assesses its material sustainability topics not in isolation but against the external risk environment. The register below maps each topic to the relevant global-risk anchor, states the associated risk and opportunity, and sets out our response. For a cybersecurity company, several of the most severe global risks are simultaneously threats to be managed and drivers of demand for the protection we provide. On the environmental side, our footprint is concentrated not in owned facilities but in the energy and carbon intensity of the cloud and IT infrastructure we rely on.

Digital Security and AI

Material Topic	Risk • Opportunity	Group-IB Response
Misinformation and deepfakes	Risk • As an information-integrity actor, any breach or misstep is reputationally amplified Opportunity • Direct demand driver: BioConfirm anti-deepfake biometrics and deepfake/vishing research cited by the FBI and the American Bankers Association	Develops and markets BioConfirm, its anti-deepfake biometric verification technology; offers Fraud Protection to detect fraudulent schemes; publishes open threat research through the Research Hub, reinforcing its reputation as an information-integrity expert
Responsible AI and dual-use	Risk • Model misuse, detection error/hallucination, and EU AI Act exposure; the same AI that empowers defenders empowers attackers Opportunity • Responsible AI position, AI Red Teaming service, and human-in-the-loop AI Assistant as differentiators while peers only declare intent	Finalizing a Responsible AI Policy for 2026; runs the AI Cybersecurity Hub to test models and monitor AI-driven threats; aligns internal processes with the NIST AI RMF and ISO/IEC 23894 standards
Cyber insecurity and supply-chain fragility	Risk • Group-IB is itself a high-value supply-chain target holding sensitive client threat data; a compromise would collapse trust Opportunity • Core demand driver: Unified Risk Platform, Representative Vendor in the Gartner Market Guide for DFIR Retainer Services, and the GDPR-compliant CFIP	Builds out its Unified Risk Platform; operates CERT-GIB, a 24/7 incident-response team; designs CFIP on privacy-by-design principles; runs its own third-party risk assessment and monitoring program
Service reliability and systemic technology risk	Risk • As a 24/7 detection and response provider to banks, government, and critical infrastructure, any outage or error in our own platforms propagates systemic risk to clients in sensitive sectors Opportunity • Demonstrated uptime, DFIR service levels, and resilience engineering become a competitive qualifier for regulated-sector clients under DORA and NIS-2	Delivers round-the-clock monitoring and incident response through CERT-GIB; maintains ISO/IEC 27001 certification; is preparing to complete a SOC 2 Type II audit by 2027-2028

Social

Material Topic	Risk • Opportunity	Group-IB Response
Cybersecurity skills shortage	Risk • Global talent scarcity constrains growth (a stated material topic); key-person dependency and retention pressure in a competitive market Opportunity • Academic Alliance, the 1,000-STEM by-2027 commitment, and the Partner Academy convert the skills gap into a talent pipeline and sovereign capability-building across Central Asia, META, and LATAM	Runs the Academic Alliance program, partnering with 15+ universities across 11 countries; operates a mentorship program to train specialists; organizes national cyberdrills, including in Kyrgyzstan

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Environmental and Climate

Material Topic	Risk • Opportunity	Group-IB Response
Energy and carbon intensity of cloud/IT infrastructure	Risk • Our footprint is dominated by Scope 3 (purchased cloud and IT services), which rose 120% in 2025 and lies largely outside our operational control Opportunity • Extending renewable procurement beyond the EU office, improving compute and model efficiency, and prioritizing low-PUE, high-renewable cloud regions cut both cost and carbon intensity; a near-term SBTi-aligned intensity target would close the peer gap	Tracks emissions under the GHG Protocol; calculates Scope 3 emissions via the Perk platform; pilots renewable-energy procurement (GreenChoice) at its EU office
Value-chain (Scope 3) data and hyperscaler dependence	Risk • Decarbonization depends on a handful of hyperscalers whose emissions we inherit; enterprise and financial-sector clients increasingly require verified Scope 3 and supplier-climate data in procurement and ESG questionnaires which we cannot yet supply Opportunity • Engaging cloud providers on renewable-matched regions and building the capability to answer client Scope 3 requests turns a data gap into a commercial qualifier for regulated-sector tenders	Calculates Scope 3 emissions using a spend-based methodology with inflation adjustment. Plans to build a system for collecting supplier climate data
Climate resilience of infrastructure and operations	Risk • Extreme weather threatens the third-party data centers and offices on which service continuity depends, concentrated across a limited set of providers and regions Opportunity • Multi-region cloud redundancy and tested continuity planning reduce outage risk and support DORA/NIS-2 obligations for financial-sector clients	Maintains business-continuity plans; hosts infrastructure across multiple regions for resilience. Plans to formalize a physical climate-risk assessment

Governance

Material Topic	Risk • Opportunity	Group-IB Response
Geoeconomic fragmentation and trust	Risk • Multi-jurisdiction footprint invites export-control and data-localization scrutiny; security vendors are state-actor targets; regulatory divergence (GDPR, DORA, NIS-2, AI Act) Opportunity • The decentralized DCRC model is a structural hedge against fragmentation (proximity, data residency); certifications (ISO, DoJ attestation, Bureau Veritas, GDPR-by-design) are trust and market-access assets	Operates a network of 11 regional response centers (DCRCs) for local presence and data residency; holds a full suite of certifications to demonstrate trustworthiness; designs CFIP on privacy-by-design principles; signs MoUs with governments to build national cyber capability

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Stakeholder Engagement

Group-IB's material topics are shaped by the organizations and people closest to our mission. For the 2025 assessment we structurally engaged the principal stakeholder groups identified in the inaugural Group-IB Sustainability Report, narrowing down the focus groups to our clients, regulators and law-enforcement institutions, business and academic partners and suppliers, employees and executive leadership.



Clients

Enterprise and government clients provided input on cybersecurity risk, data protection, and service reliability through feedback channels and ESG questionnaires.



Regulators and law-enforcement institutions

Engagement helped align our priorities with legal, ethical, and cross-border cooperation standards.



Business partners and suppliers

Input addressed supply-chain integrity and third-party risk.



Academic partners

Collaboration informed our view on workforce development and emerging technology risk.



Employees

Internal consultations with cybersecurity analysts, engineers, and compliance teams surfaced operational and security-related priorities.



Executive leadership

Management weighted topics against strategic relevance and long-term goals.

04

Environment and Climate

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Measuring Our Climate Impact

Group-IB laid the baseline for our greenhouse gas (GHG) emissions calculations in our inaugural Sustainability Report 2024, and committed to calculating them annually going forward, because we believe that measurement and transparency are the foundations of accountability. This process allows us to interpret our performance year over year, identify where operational efficiency can be improved, and manage the climate-related risks inherent in operating a global cybersecurity business. As we scale, we treat emissions reporting not as a compliance exercise but as a core component of operational resilience.

As a cybersecurity firm, our environmental footprint originates from a defined set of sources. The largest contributors are the IT infrastructure and server capacity, which gives us a precise view of where impact concentrates and where mitigation efforts can be most effective.

Methodology and Data Quality

Our emissions in 2025 are calculated in line with standard carbon accounting frameworks, such as **the GHG Protocol.** For this reporting cycle, we integrated two methodological refinements designed to improve the precision of our calculations.

First, we optimized our **emission factors.** In 2024, factors were predominantly modeled using broad datasets from the UK Department for Business, Energy & Industrial Strategy (BEIS). For 2025, wherever localized country-specific data became available, we transitioned from BEIS to corresponding national grid and regional sources. This adjustment materially enhances geographical precision, though we note transparently that it introduces inherent structural variances when evaluating annual trends.

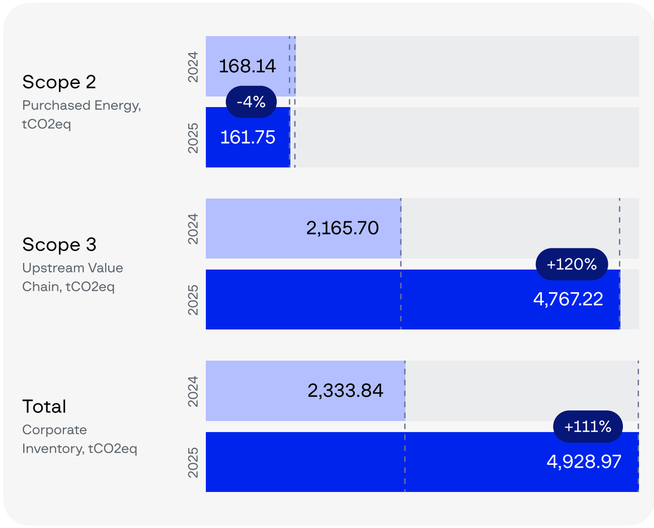
Second, for upstream **Scope 3** categories calculated using a financial spend-based methodology, we applied an inflation control. To prevent macroeconomic inflation from artificially inflating our calculated impact, all 2025 expenditure figures were deflated back to 2024-equivalent dollars, and historical 2024 emission factors were applied against these adjusted figures. As a result, the reported changes reflect genuine physical purchasing volumes and commercial activity rather than shifting market dynamics.

Emissions Breakdown

Scope 1 — Direct emissions
Scope 1 covers direct emissions from sources we own or control, such as fuel combustion in company vehicles, on-site generators, and refrigerants in office cooling systems. Because the substantial majority of our facilities are leased or shared workspaces outside our direct operational control, we have assessed our Scope 1 emissions as immaterial to our overall footprint. They are therefore not separately quantified in this inventory, which is consolidated on a Scope 2 and Scope 3 basis.

Scope 2 — Purchased electricity, heat, and steam
Scope 2 tracks the indirect emissions associated with purchased electricity and thermal energy across our global office network. In 2025, Scope 2 emissions **decreased 3.8%,** from **168.14 tCO2eq** to **161.75 tCO2eq,** mostly reflecting improvements in localized grid efficiency. Operational energy consumption remains concentrated within our core regional offices, with tracking distributed across **Europe, META, Latin America, Southeast Asia, Singapore, and Uzbekistan.**

Scope 3 — Upstream value chain
Scope 3 captures indirect emissions across our broader value chain, specifically purchased goods and services, business travel, and employee commuting. In 2025, upstream emissions rose from **2,165.70 tCO2eq** to **4,767.22 tCO2eq,** an increase of **120%.** This expansion was driven primarily by two factors directly tied to the active growth of the company: increased procurement and spending on IT infrastructure and services required to support the adoption of AI technologies across our operations, and higher business travel activity necessitated by our expanding global footprint and market presence.



Growth and Mitigation

We report an absolute increase in our total corporate carbon inventory, from **2,333.84 tCO2eq** in 2024 to **4,928.97 tCO2eq** in 2025, a rise of **111%.** We address this transparently: the increase coincides directly with a period of rapid business expansion, geographic growth into new markets, scaling workforce and increased penetration of AI. As commercial activity, infrastructure investment, and travel intensify to meet customer demand, our footprint has grown alongside them.

We recognize that absolute growth in emissions is not an acceptable long-term trajectory, and our objective is to decouple business growth from planetary impact, so that future expansion is achieved with progressively lower carbon intensity. Two efforts anchor this work.

First, we are transitioning to **renewable energy** where it is operationally feasible. At our European office we continue sourcing lower-carbon electricity through GreenChoice, our renewable energy supplier, establishing a model we intend to extend across our office network as local market conditions allow.

Second, we have deployed **Perk,** a travel booking platform, to deeply understand, track, and optimize our Scope 3 emissions, with particular focus on business travel, the most significant and most addressable component of our value-chain footprint. By giving our teams granular visibility into the emissions associated with individual travel decisions, Perk, through its Green Trip API, enables them to make optimal, low-carbon choices wherever possible, embedding emissions awareness directly into day-to-day operational decision-making.

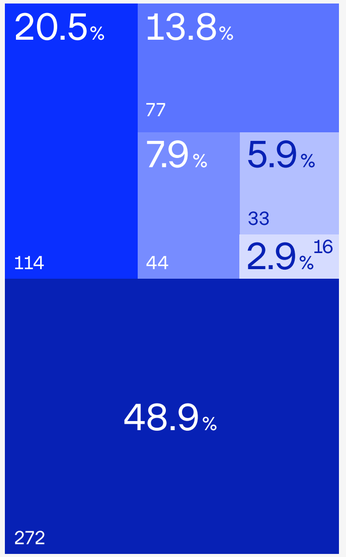
05

Social

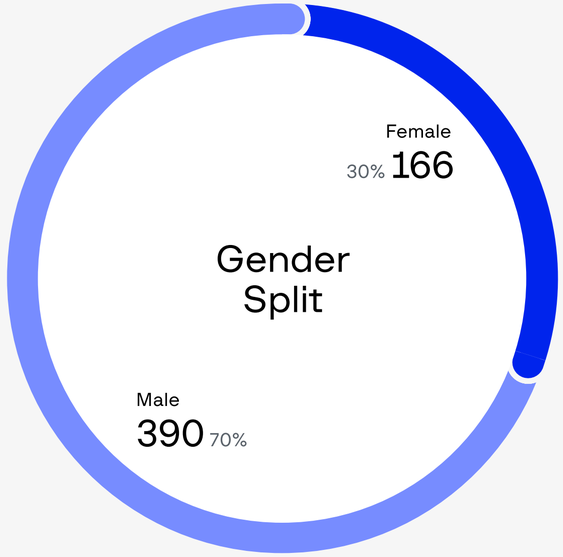
01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

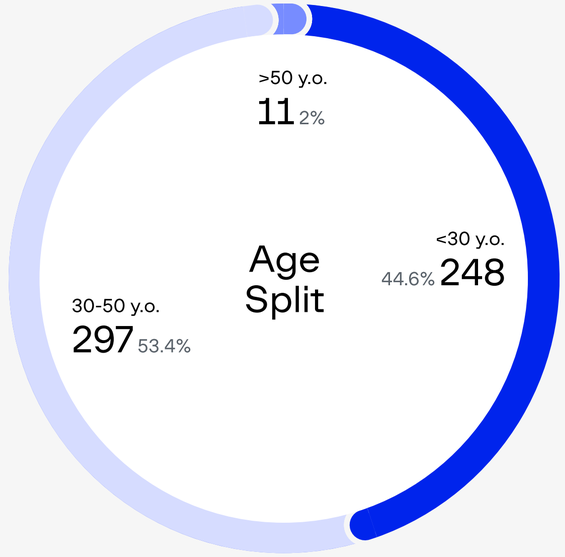
556 Employees	+25% Growth in employees vs 2024	11 Offices	60 Countries	20+ Languages	77 000+ hours Cyber incident response
32 hours Training per employee	60+ Countries served	Soft Skills Camp Launched	Mentorship Program Launched	100% Employees who received performance and career-development reviews	0 Recordable injuries or fatalities

Regional Split



— Singapore
— Uzbekistan
— UAE and KSA
— Thailand
— the Netherlands
— Chile





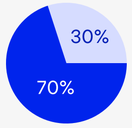
01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Our Workforce

Our team is the foundation of the company's success. Across every region of our presence, we provide the conditions for our people to work, perform, study, and grow. Investing in human capital is both a cultural commitment and an operational necessity for an organization whose mission depends on specialized, current expertise.

In 2025, the HR leadership function matured into a dedicated role at the company. This role is performed by the Chief Human Resources Officer, who reports to the CEO and manages talent acquisition, internal culture, employee development, and HR policy development. The function is also embedded in our ESG governance through direct involvement in shaping internal culture initiatives, organizing company-wide events, and developing and communicating people-related policies — ensuring that workforce strategy and inclusive governance inform company-wide commitments.

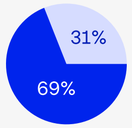
In 2025, Group-IB operated in **60 countries** through **11 offices** with **556 employees** and contractors, representing **25% growth** compared to 2024. Of this total, **70% represented R&D and technical roles,** reflecting our sustained commitment to research and the continuous implementation of new technologies in service of our mission to fight cybercrime.



Combined Global Workforce

556 professionals

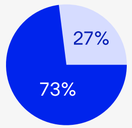
— Male (390) — Female (166)



Core Permanent Full-Time Layer

308 professionals

— Male (209) — Female (99)



External Contractor Layer

248 professionals

— Male (181) — Female (67)

Employment Structure

During the 2025 reporting period, Group-IB successfully onboarded 180 new employees, reflecting continuous corporate growth. Broken down by gender, the new hire intake comprised 120 male and 60 female professionals. From an age demographic perspective, the company's recruitment pipeline remained heavily anchored in highly active mid-level and emerging technical brackets, onboarding 88 individuals aged 30–50 and 81 individuals under the age of 30. Strategic senior expertise and leadership pathways were further reinforced by the addition of 11 professionals in the 50+ age category.

During the 2025 reporting period, Group-IB recorded a total of 63 employee departures across its regional operations. Broken down by gender, the group-wide employee turnover layer comprised 41 male and 22 female professionals. From an age demographic perspective, departures were primarily concentrated within emerging and mid-level operational brackets, accounting for 33 individuals under the age of 30 and 28 individuals aged 30–50. Turnover among senior-level tiers remained exceptionally low, logging just 2 professionals in the 50+ age category.

Leadership and Remuneration

Group-IB's approach to leadership and remuneration reflects its broader commitment to building a sustainable, globally distributed organization. As the company scales its Digital Crime Resistance Centers across seven operational hubs, it is equally focused on cultivating the leadership bench and compensation practices needed to support that growth responsibly — from the gender and age composition of its regional executive teams to the wage standards applied across every market in which it operates.

The demographic composition of Group-IB's regional top management tier across its global operating centers reflects a structured distribution of leadership across key age and gender brackets. Across the localized executive management positions in the company's seven operational hubs, the gender breakdown consists of 19 male executives and 5 female executives.

From an age distribution perspective, this leadership layer is heavily anchored by experienced mid-career professionals, with 21 executives falling within the 30–50 age bracket, 2 executives under the age of 30, and 1 executive in the 50+ category, with the concentration of younger leaders reflecting fast-track leadership development in emerging hubs like Uzbekistan. This executive structure provides a highly stable blend of mature industry expertise and localized operational agility across all regional DCRCs.

Providing competitive and equitable compensation is a foundational element of our human capital strategy. Group-IB aligns its entry-level wages with specialized industry engineering benchmarks, ensuring that compensation across all operational regions consistently exceeds both local statutory minimums and standard market averages. In 2025, **100% of employees received performance and career-development reviews.**

Health and Safety

We recorded **0 injuries, fatalities, and cases of ill-health** across our operations, consistent with the low-risk profile of our work and our duty-of-care standards.

Engagement, Grievance, and Whistleblowing

We sustained workforce cohesion through internal sports, volunteering, and retreat events over the year. To protect a fair and accountable workplace, all employees have access to formal channels for grievance and whistleblowing via internal and external channels, enabling concerns to be raised confidentially and addressed through defined procedures. The procedure is regulated by the new Code of Conduct ↗ (more details in section Governance).

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Training and Talent Development

Group-IB treats employee development as a component of operational resilience: in a threat landscape that changes continuously, the value of our workforce rests on current, verifiable expertise. In 2025 we introduced a structured curriculum spanning company-wide onboarding, role-specific commercial and technical enablement, and team-level capability building, delivered in part through the Group-IB Academy on the LearnUpon platform.

We have also launched the Soft Skills Menu, an internal library of development programs that allows each team to select an intervention matched to its specific objective rather than a standardized course. Available formats include team diagnostics, team building, targeted skills training, psychotype-based diagnostic games, strategic sessions, knowledge-sharing, and custom formats. Topics span communication and conflict management, networking, public speaking, cross-cultural collaboration, career coaching, stress management, and decision-making.

Academic Alliance

The Group-IB Academic Alliance is the company's flagship education and capacity-building program, partnering with universities to embed advanced cyber technology and current defense practice directly into the classroom. The Alliance co-develops programs that pair academic rigor with operational expertise, giving students the same investigative and analytical experience used by practitioners. Each partnership is tailored to regional languages, regulations, and threat landscapes, and is reinforced by a Train-the-Trainer model that certifies professors as instructors — ensuring the capability scales sustainably within institutions rather than depending on Group-IB alone. As an ESG social output, the Alliance is a direct response to the global cybersecurity skills gap: it converts the company's threat intelligence and tooling into durable workforce capacity and stronger regional digital resilience.

In 2025, the Alliance expanded from 6 to 15+ partnerships across 11 countries, with a cohort of 400+ students passing through the formalized program tracks.

New university partnerships include:

- CSU (Cyber University), Uzbekistan
- Mahidol University, Thailand
- National Polytechnic University, Armenia
- Nebrija University, Spain
- LISA Institute, Spain

Beyond universities, the Alliance's capacity-building model extended to national and regulatory institutions to support national cyber defense, including BOCRA (Botswana Communications Regulatory Authority) and the Ukuk platform in Kyrgyzstan.

Program	Audience	Format & Timing	Key Topics
Products & Services Overview (LearnUpon / Group-IB Academy)	All employees without exception — "newcomers, veterans, techies, and non-techies alike"	11–12 short lessons on LearnUpon; non-technical overview	Group-IB's mission and global presence, threat types, products, the Unified Risk Platform, services and investigations, and support for law enforcement
Revenue Cloud Advanced (CRM tool)	BDM, Pre-Sales, Coordinating, Product/Service Management, and Finance	Rollout October 2025	New CRM quoting tool plus product updates across Fraud Protection, ASM-TI-DRP, and MSSP
META Sales Enablement Bootcamp	New Sales hires in the META region	Four-day onboarding, early November 2025	MSSP, Services, MXDR, Channels, Fraud Protection, URP, Investigations, Marketing, Salesforce, plus business simulations

15+ University partnerships

11 Countries represented

40+ Professors involved: all certified each year

400+ Students reached in 2025*

4 Training languages



[*] — across programs including student-operated SOCs, the Threat Intelligence Academy, CTF competitions, and internships.

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Group-IB Hubs

Group-IB's public-facing knowledge platforms, the Research Hub and the Knowledge Hub, operationalize the company's commitment to cybersecurity knowledge sharing. Both hubs treat our industry-specific knowledge as a public good, distributing it to the wider industry, regulators, law enforcement, and the general public to raise awareness and strengthen collective digital resilience.

The Research Hub serves as our central repository for comprehensive threat analyses, trend reports, blogs, and white papers, presenting cybercrime trends to the public and the broader security community on a continuous basis. Its purpose is to convert proprietary investigative data into shared situational awareness that defenders worldwide can act on.

Alongside our flagship High-Tech Crime Trends Report, Group-IB published 43 technical research blogs ↗, freely available research that other companies, regulators, and law-enforcement bodies use to reduce the societal cost of cybercrime — an indirect but measurable economic benefit.

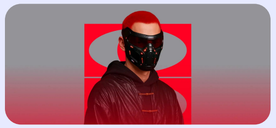


High-Tech Crime Trends Report 2026 ↗

Built on the analysis of 1,540+ investigations, documented a 58% increase in APT-attributed attacks and was widely covered by leading media outlets globally.



UNC2891 Bank Heist (banking • ATM intrusion) ↗



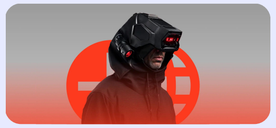
ShadowSilk (Central Asia • APAC threat actor) ↗



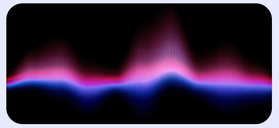
MuddyWater Espionage Campaign ↗



RansomHub Never Sleeps: Episode 1 ↗



Hunters International Ransomware Group ↗



Deepfake Voice Phishing (Vishing Anatomy) ↗



The Cybercriminal with Four Faces (ALTDOS) ↗



Deepfake Fraud (biometric • KYC bypass) ↗

Podcasts

In 2025 Group-IB launched two public podcast series ↗, publishing 12+ episodes in total and extending its education activity into new channels:



Masked Actors ↗
10 episodes
Launched 13 May 2025
Based on the HTCT 2025 report

Hosted by Gary Ruddell and Nicholas Palmer, each episode profiles one of the year's top-10 cybercriminal groups (including GoldFactory, Lazarus, RansomHub, MuddyWater & OilRig, Brain Cipher, and AJINA). The campaign received coverage in Forbes, VTM, and other tier-1 media.



Fraud Intel ↗
2 episodes
Launched 04 August 2025

"Unmasking Cyber Fraud in the Middle East and Beyond"
"Evolving Defense Tactics Against Rising Authorized Fraud"

Employee Voice

Individual contributions of our professionals were elevated to global standards. Sharmine Low, Malware Analyst, and Nam Le Phuong — Senior Digital Forensics and Incident Response Specialist, APAC, contributed to MITRE ATT&CK v17, the cybersecurity industry's most widely adopted knowledge base of adversary tactics and techniques, built from real-world observations and used globally by defenders to detect, classify, and respond to attacks. Due to its nature as a community-curated standard, accepted contributions to it are rare and externally validated. This translates into a direct, attributable mark of our technical credibility on the world stage.

> It was an unexpected finding and ultimately did lead to some form of contribution to the community. It is also a good reminder that fresh eyes and curiosity can sometimes lead to interesting finds.
>
> Sharmine Low
> Malware Analyst, APAC

> In Incident Response you're constantly seeing attacker techniques that predate whatever's written down in the public frameworks, because you're reconstructing what actually happened on a compromised system, not reading about it after the fact. Most of that knowledge stays inside case notes and never goes further. Turning part of it into a contribution to ATT&CK v17 meant that observation didn't just help close one case, it's now part of how analysts everywhere classify and respond to similar attacks.
>
> Nam Le Phuong
> Senior Digital Forensics and Incident Response Specialist, APAC

Over the year, Anastasia Tikhonova, Technical Head, APAC, co-authored the threat report on UNC2891, a financially motivated threat actor that specializes in deep intrusions against banking and ATM infrastructure. She also spoke at High-Tech Crime Trends 2025 across six regions, was interviewed by CRN Asia at GovWare, the anchor conference of Singapore International Cyber Week and Asia's premier cybersecurity event, presented at the 8.8 Conference in Santiago, Latin America's foremost technical security conference, and served as a mentor in our corporate program.

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

> In 2025, I tried to rethink how we present our research and threat intelligence, and a key idea behind the High-Tech Crime Trends Report 2026 was bringing more connectivity into how we describe threats — a single compromise rarely exists in isolation, and our intelligence should help people see those connections. I took a similar approach co-authoring our research into UNC2891, aiming not just to document the intrusion but to show how its parts worked together, giving financial institutions something concrete to check against their own environments. Presenting across six regions meant preserving that substance while making it relevant to each audience.
>
> Anastasia Tikhonova
> Technical Head, APAC

At the Top Women in Security ASEAN Region Awards 2025 — part of the global Women in Security & Resilience Alliance (WISECRA) campaign, now in its sixth year — Group-IB investigators won two country awards and reached the finalist shortlist.



Hai Ha Phan
Cyber Investigation Specialist
Country Award winner, Vietnam



Jessica Tedja
Cyber Investigation Specialist
Country Award winner, Singapore



Vesta Matveeva
APAC Head of High-Tech Crime Investigations
Top 20 finalist

These recognitions reflect a deliberate practice of giving employees visible platforms for their expertise and perspective, strengthening both engagement and the company's standing in the wider security community.

Community Engagement

For Group-IB, community engagement is a deliberate investment in human capital on which our long-term operational resilience depends. In 2025, we engaged with the next generation of cybersecurity professionals, national institutions we partner with, and communities where our teams live and work, across multiple, mutually reinforcing channels.

Mentorship Program

Group-IB launched its first structured corporate Mentorship Program, which serves as a cornerstone of our human-capital strategy and our most direct mechanism for transferring institutional expertise to the next generation of professionals. The technical track pairs junior- and middle-level specialists one-on-one with senior colleagues to develop professional skills directly within the working context. The program is fully integrated into our HiBob platform, ensuring a transparent, scalable, and auditable matching process. A leadership track is planned as the next phase, extending the same knowledge-transfer model to employees pursuing management growth.

Soft Skills Camp

Our Soft Skills Camp complements technical mentorship by building the communication and leadership capabilities essential to a modern professional workforce. The Camp helps employees master the essentials of effective communication, leadership, and workplace navigation. It introduced a dedicated public-speaking stream, recognizing that strong communication is a daily skill critical for business. Participants gained access to a self-paced public speaking course offering practical techniques and frameworks, alongside personalized 1:1 coaching sessions to prepare for meetings, presentations, and events.

Operating in many regions of the world, we also understand the importance of cross-cultural fluency. To explore regional business ethics, professional conduct, effective meetings, trust-building with local clients, and feedback norms, the Saudi Arabia office hosted a multicultural "Saudi Insights" event, where 30 team members co-created a practical regional guideline as a lasting output.



GISEC Global 2025 (UAE)

Group-IB leveraged this premier event to sign several strategic regional Memorandums of Understanding across META to expand its regional market reach. Additionally, Group-IB was recognized on a government level, receiving the "Outstanding Partner" award from the UAE Cybersecurity Council at the conference.









8.8 Computer Security Conference

Group-IB participated in the 15th anniversary edition of this conference, which is one of the most prominent cybersecurity events in Latin America. The technical team presented to more than 750 attendees, sharing the latest trends in global cybercrime and outlining proactive targeted threat interception strategies using Threat Intelligence. Anastasia Tikhonova (Technical Head, APAC) traveled to Santiago as a key speaker for this event.





01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Black Hat MEA 2025

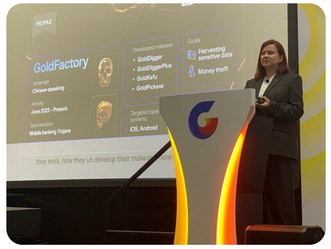
The company maintained an active presence at the conference, deploying booth infrastructure and an on-the-ground regional advisory team.



GovWare

Group-IB engaged with industry circles at GovWare, where Anastasia Tikhonova represented the company and provided a featured technical interview for CRN Asia.







Digital Kyrgyzstan 2025 National Cyberdrill

Moving beyond standard event attendance, Group-IB served as the cornerstone private sector technical partner and co-organizer of this nationwide initiative. Conducted in partnership with the Ministry of Digital Development and Innovation Technologies of the Kyrgyz Republic, the OSCE Programme Office in Bishkek, and the International Telecommunication Union (ITU) Regional Office for the CIS, the drill served as the country's largest collaborative platform for regional cybersecurity community knowledge-sharing.





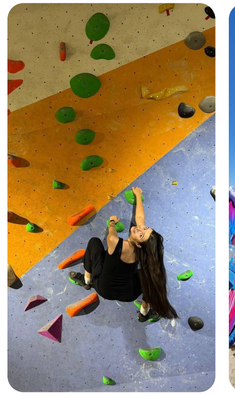


Volunteering for the Common Good

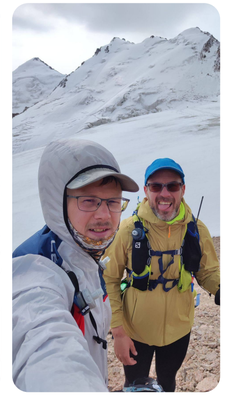
Our people translate corporate values into tangible community support. During Ramadan in March 2025, employees in our Dubai office organized a charity drive, collecting goods for those in need — an employee-led expression of the solidarity and social responsibility that underpin our culture.

Sports & Wellness Initiatives

Group-IB treats physical wellbeing and team cohesion as integral to a healthy, high-performing organization. In August 2025 we held "Group-IB Goes Distance," our annual company-wide sports challenge. The momentum carried into November, when winning participants from our Central Asia teams traveled to compete in the picturesque races of Samarkand, proudly carrying the Group-IB flag across the finish line near Registan Square before exploring the region's cultural heritage. The initiative celebrated teamwork, dedication, and community integration through a shared, milestone-driven experience.







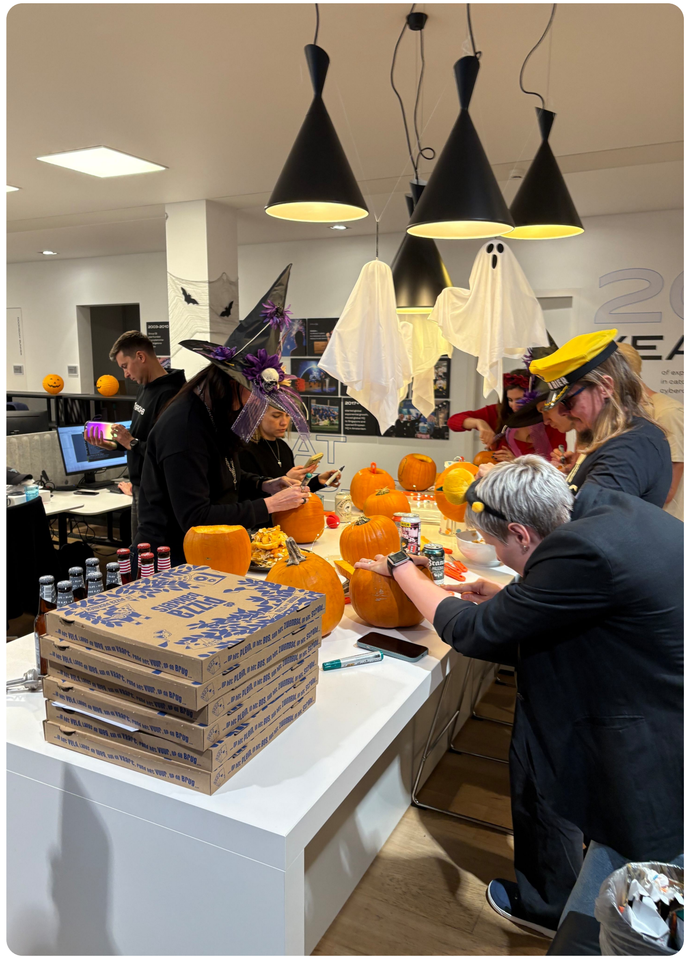


01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Corporate Culture & Internal Celebrations

Finally, we cultivate community inside the organization, recognizing that an engaged internal culture is the foundation of every external commitment. In September 2025, our Chilean team celebrated Chile's Independence Day (Fiestas Patrias) with traditional music and asado, while members of our finance team in Tashkent explored local bazaars, artisan crafts, and landmarks, surfacing shared themes of heritage and family. October brought Halloween pumpkin team-building events across offices.

We also invest in onboarding as culture-building: in November, new Sales team members in the META region completed a four-day enablement bootcamp combining deep-dive strategy sessions, live business simulations, and cross-regional networking. Through these celebrations, cultural milestones, and team events, we nurture the sense of belonging that empowers our people to extend resilience and goodwill outward to the communities we serve.











06 Governance

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

At Group-IB, robust corporate governance is foundational to our organizational resilience and strategic execution. We embed the same operational disciplines required to defend global digital infrastructure, such as accountability, risk controls, and continuous oversight, directly into our corporate leadership framework. By aligning our internal governance architecture with the exacting standards of our cybersecurity operations, we ensure transparent, ethical decision-making, rigorous compliance, and sustainable value creation for all stakeholders.

In 2025, we continued to maintain a high degree of financial autonomy. Across almost all jurisdictions in which we operate, no government subsidies, grants, or direct financial assistance were requested or received. The sole exception was our global headquarters in Singapore, where, under active national business and workforce support schemes for personnel on official labor contracts, the company recorded government payouts and compensation.

These inflows were allocated across the following targeted programs:

- **Progressive Wage Credit Scheme,** aimed at supporting local human capital development and co-funding baseline wage increments.
- **Corporate Income Tax Rebate,** as part of nationwide economic stimulus measures designed to reinforce corporate operational resilience.
- **National Service Reimbursements,** an official statutory reimbursement from the government to cover employer costs for wages paid to core staff members during their absence from work while fulfilling mandatory regular reserve military service training cycles in Singapore.

These accruals reflect Group-IB's structural integration into the economic ecosystem of Singapore, the transparency of its corporate tax accounting, and its strict compliance with local labor and civic regulations.

Board of Directors

Group-IB's organizational structure remained stable through 2025, with no recorded changes since 2024. No board appointments, departures, role changes, or committee-structure changes occurred during the reporting period, reflecting continuity of leadership through a year of sustained business growth.

The Board of Directors comprised five members, all of whom served in executive capacities, with its composition remaining entirely male. Collectively, directors contribute expertise spanning cybersecurity, management, legal, finance, technology, and entrepreneurship.

The Board convened four times on a quarterly cadence. Quarterly sessions reviewed the company's operational and performance data, while the additional annual meeting was dedicated to approving the budget and business strategy for the year ahead.

Dmitry Volkov, Co-Founder and CEO, continued to serve as Chairman of the Board. As the company scales across new markets, Dmitry's operational depth and sector expertise remain integral to the unified leadership the Chairman role demands.

> Stability in governance is what allows Group-IB to grow with confidence. Over the past year, our Board has given us a steady foundation as we've expanded into new markets. As Chairman, my responsibility is to make sure that stability translates into disciplined oversight, reviewing our performance rigorously each quarter and setting a clear strategic direction each year. Sustainability, to me, is an extension of that same discipline: building a company, and an industry, that holds up over the long term. That means responding to the evolving cyberthreats and fraud that threaten the stability and continuity of businesses worldwide.
>
> 
> Dmitry Volkov
> CEO and Co-Founder, Group-IB

ESG Management

ESG matters reaching the Board agenda during the year include environmental disclosures, human capital, research and development, regulatory compliance, AI governance, and supplier due diligence, amongst others. Accountability for these themes rests with Deputy CEO Anastasiia Komissarova, who chairs a cross-departmental ESG Working Group and reports directly to the Board of Directors. Further detail on ESG oversight is provided in the section ESG at Group-IB ↗.

Code of Conduct, Ethics and Anti-Corruption

In 2025, Group-IB published a new Code of Conduct ↗. This cornerstone document establishes the ethical baseline for every employee, board member, and business partner, with global reach across all DCRCs, branches, and affiliates regardless of jurisdiction.

Following a coordinated internal and external rollout of the CoC:

- **100% of employees and Board members** completed CoC and anti-corruption training and acknowledgement
- The CoC was extended to **100% of business partners**

Governance highlights

100%

Employees, BoD members, and partners acknowledge the new Code of Conduct

Zero

Incidents of corruption	Losses of customer data
Breaches of customer privacy	Legal actions related to anti-competitive behavior
Cases of whistleblowing	Cases of Ethics Hotline reports



Code of Conduct ↗

Ethical guidelines and professional standards to ensure integrity, confidentiality, and responsible behavior

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

The CoC establishes clear whistleblowing channels:

- Internal escalation through an employee's direct manager, Chief Regional Officer, HR Business Partner, Chief Security Officer, or Legal team.
- A public channel via codeofconduct@group-ib.com.

Non-retaliation protection is provided for all good-faith reports, even where a concern is ultimately unsubstantiated. In 2025, 0 such concerns were raised.

Group-IB sustained its zero-tolerance stance on discrimination, bribery, corruption, and workplace violence. Consistent with 2024, the company recorded 0 confirmed incidents of corruption and 0 legal actions related to anti-competitive behavior. The Ethics Hotline — a confidential resource introduced under the internal "Feedback Culture" project for reporting ethical concerns, misconduct, or policy violations — received 0 reports during the year. We regard the availability and awareness of these channels as a measure of a healthy, transparent culture, and we communicate them consistently across the organization and partner network.

Data Privacy and Compliance

For Group-IB, information security and data privacy are not isolated compliance requirements; they are central to our enterprise risk management framework and foundational to stakeholder trust. We treat data protection as our paramount governance asset, safeguarding our operations and client information through an independently audited control environment that is continuously certified against global security standards.

Certifications and Frameworks

The company's standing as an audited, trusted partner is reflected in its formal relationships with INTERPOL, EUROPOL, and AFRIPOL, its cooperation with the U.S. Department of Justice, and its GDPR-aligned data protection framework. For relevant European clients, the compliance program addresses the Digital Operational Resilience Act (DORA, effective January 2025) and the NIS-2 Directive.

Group-IB's Privacy Policy ↗ is published online, with Group-IB Global Private Limited (Singapore) as data controller. It covers the EU GDPR and Singapore PDPA and sets out the full schedule of data-subject rights.

Our Code of Conduct codifies personal data processing obligations for all employees. In 2025, the company recorded 0 substantiated complaints concerning breaches of customer privacy and zero losses of customer data.

ISO/IEC 27001:2022

Information Security Management (TÜV AUSTRIA)

Applus+ ENS-High

Spanish National Security Framework

ISO 9001:2015

Quality Management (TÜV AUSTRIA)

SOC 2 Type II

Planned for 2027-2028

GDPR

Compliance, alongside regional data-protection laws (PDPA, PDPL, and others)

EU AI Act

Alignment planned, implementation in 2026

Responsible AI Policy

In 2025, Group-IB formalized its approach to AI governance, articulating a public Responsible AI position, with a formal public AI Governance Policy slated for publication in 2026 subject to Board endorsement.

The AI Cybersecurity Hub ↗ currently operates on the principles of Explainable AI (XAI) and human-in-the-loop oversight, aligned with the NIST AI RMF, ISO/IEC 23894:2023, and the EU AI Act, and is positioned as a Responsible AI resource.

The framework is operationalized across products and services:

- AI Red Teaming — offered as a service to help clients test the security of their own AI systems.
- AI Assistant (beta, April 2025) — an LLM-powered chatbot within the Threat Intelligence platform, built to augment analysts rather than replace them.
- Prevyn AI, launched in May 2026 — the cognitive core of Group-IB's Unified Risk Platform, designed to move security from reactive to predictive. Powered by Group-IB's proprietary Intelligence Data Lake built from decades of cybercrime investigations, it coordinates specialist AI agents to identify attacker intent before attacks launch and assists analysts in alert investigation and response. Human-in-the-loop is architectural — every AI recommendation requires human approval before execution — reflecting Group-IB's commitment to responsible AI development aligned with emerging global governance standards.

Human Rights

Group-IB addresses human rights directly in its Code of Conduct, which applies to all employees, Board members, and business partners. It maintains zero tolerance for discrimination on the basis of race, gender, age, religion, origin, sexual orientation, disability, or political views, and bases all employment decisions strictly on objective criteria such as skills, qualifications, and results. All forms of harassment, bullying, and physical or verbal violence are prohibited.

To keep these commitments active in daily practice, the internal "Feedback Culture" project gathers feedback on a regular basis, including through anonymous submissions. It gives employees a consistent way to raise concerns and propose ideas, many of which have led to practical improvements across the Company.

Supply Chain and Procurement

Our approach to supply chain resilience and third-party risk management is governed by our Code of Conduct, which establishes strict ethical and operational standards for all vendors and business partners. This comprehensive framework enforces rigorous oversight throughout the procurement lifecycle, serving as the strategic foundation for our mandate to achieve 100% supplier screening by 2026.

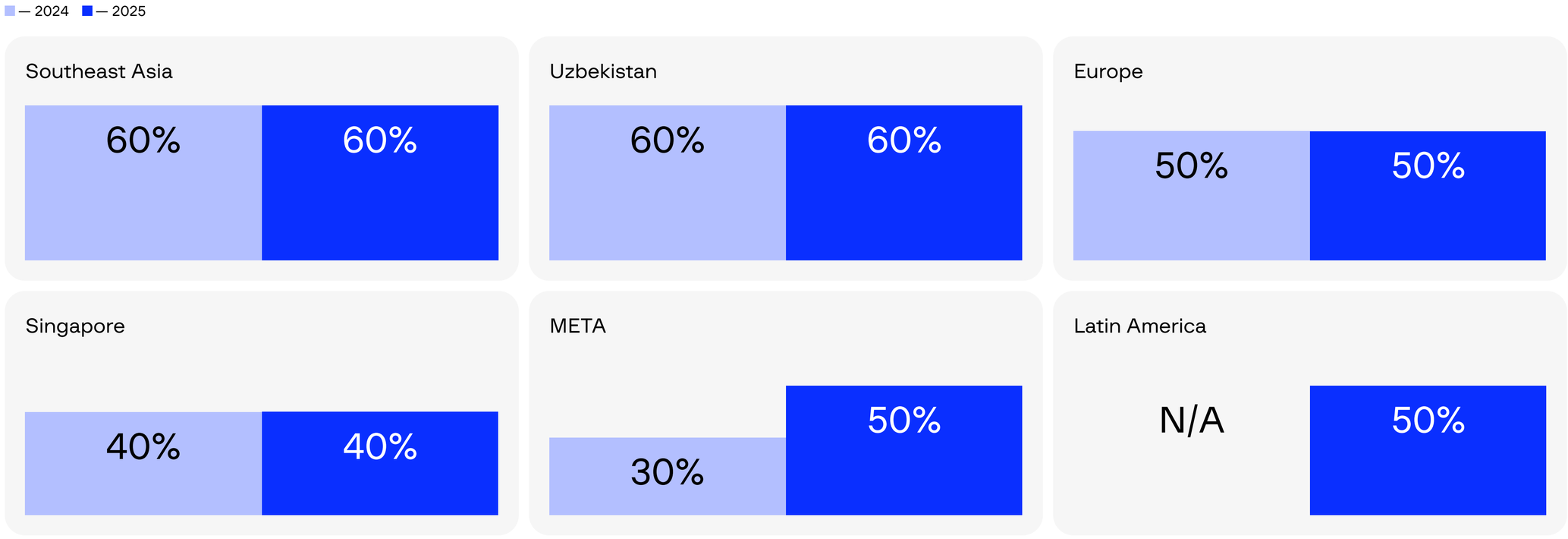
As a global provider of threat intelligence and cybercrime resistance solutions, Group-IB's procurement baseline is heavily driven by digital technology assets rather than physical raw materials. At our global headquarters in Singapore (40% local) and our European office in the Netherlands (50% local), significant capital is deployed into multi-region hyperscale cloud networks, globally distributed data pipelines, and specialized threat-intel extraction tools. Because these top-tier data ecosystems are heavily consolidated among a few international tech providers, they naturally inflate the international sourcing share.

Conversely, operating hubs like Thailand (60% local) demonstrate highly successful integration with regional corporate networks. Local spending in these theaters is primarily directed toward regional software engineering contractors, localized network access providers, domestic data centers, and regional professional services. This deliberate sourcing approach reinforces operational resilience by minimizing localized supply chain vulnerabilities.

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

Moving forward, Group-IB aims to continually audit its supplier network to identify opportunities for regional substitution, particularly within facility operations, hardware provisioning, and administrative services. This approach ensures that as our regional centers scale in headcount and market footprint, our positive economic impact on localized communities scales in parallel.

Local-supplier spend by region



07

Appendices

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

GRI Content index

GRI Disclosure	GRI Standard	Report Page Reference	Direct Information / Scope Notes
GRI 2: General Disclosures 2021	2-1 Organizational details	pp. 04, 06, 07	HQ in Singapore (Group-IB Global Private Limited); 11 Digital Crime Resistance Centers
	2-2 Entities included in sustainability reporting	p. 04	• Group-IB Global Private Limited (Singapore) — HQ • Group-IB Europe B.V. (Netherlands) • Group-IB MEA FZ-LLC (UAE) • Group-IB Consultoría LATAM Limitada (Chile) • Group IB Gulf Limited (Single Person Company) (Saudi Arabia) • Group IB Management Regional Head Quarter (Saudi Arabia / RHQ) • LLC Group-IB TSHK (Uzbekistan) • Group-IB SEA Co. Ltd (Thailand)
	2-3 Reporting period, frequency and contact point	pp. 01, 04, 34, 42	Calendar year 2025 (1 Jan – 31 Dec 2025); annual cadence; reporting contact via codeofconduct@group-ib.com
	2-4 Restatements of information	pp. 04, 23	Refinement of emission factors (BEIS to national grid datasets) and spend deflation for Scope 3
	2-5 External assurance	p. 04	No external limited assurance conducted for the 2025 reporting cycle
	2-6 Activities, value chain and other business relationships	pp. 06, 08, 09, 34	Intelligence-driven cybersecurity platforms, DFIR services, and tech supply-chain profile
	2-7 Employees	pp. 07, 25, 26	556 global workforce; 308 permanent employees (200 male, 108 female)
	2-8 Workers who are not employees	p. 26	248 external contractors (209 male, 99 female)
	2-9 Governance structure and composition	pp. 18, 33	Board of Directors comprising 5 executive members (all male)

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

GRI Content index

GRI Disclosure	GRI Standard	Report Page Reference	Direct Information / Scope Notes
GRI 2: General Disclosures 2021	2-10 Nomination and selection of highest governance body	p. 33	Unchanged board structure with no new appointments or committee reconfigurations in 2025
	2-11 Chair of the highest governance body	p. 33	Dmitry Volkov serves as both Chief Executive Officer and Chairman of the Board
	2-12 Role of highest governance body in overseeing impacts	pp. 17, 18, 33	Quarterly Board reviews of ESG performance indicators, targets, and external risks
	2-13 Delegation of responsibility for managing impacts	pp. 17, 18, 33	Executive oversight delegated to Anastasiia Komissarova (Deputy CEO) and the ESG Working Group
	2-14 Role of highest governance body in sustainability reporting	pp. 17, 18, 33	Quarterly operational review and strategy/target approvals by the Board of Directors
	2-16 Communication of critical concerns	pp. 17, 18, 33, 34	Direct board escalation channel; zero critical whistleblowing alerts recorded in 2025
	2-19 Remuneration policies	p. 26	Entry-level engineering benchmark exceeding statutory local minimums
	2-22 Statement on sustainable development strategy	p. 03	Joint statements from CEO Dmitry Volkov and Deputy CEO Anastasiia Komissarova
	2-23 Policy commitments	pp. 06, 14, 33, 34	Code of Conduct, Privacy Policy, and Responsible AI governance principles
	2-24 Embedding policy commitments	pp. 17, 33, 34	100% employee and partner compliance training on the updated Code of Conduct
	2-25 Processes to remediate negative impacts	pp. 26, 33, 34	Whistleblowing channels, escalation pathways, and non-retaliation protections

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

GRI Content index

GRI Disclosure	GRI Standard	Report Page Reference	Direct Information / Scope Notes
GRI 2: General Disclosures 2021	2-26 Mechanisms for seeking advice and raising concerns	pp. 26, 34	Internal manager escalations, Ethics Hotline, and codeofconduct@group-ib.com
	2-27 Compliance with laws and regulations	pp. 04, 33, 34	Zero incidents of regulatory non-compliance, anti-trust litigation, or competitive legal actions
	2-28 Membership associations	pp. 09, 12	Participation in FIRST, APCERT, OIC-CERT, APWG, Trusted Introducer, and WEF Cybercrime Atlas
	2-29 Approach to stakeholder engagement	p. 21	Structured consultations with clients, LEAs, academic partners, regulators, and employees
GRI 3: Material Topics 2021	3-1 Process to determine material topics	pp. 18, 21	Four-pillar materiality matrix process incorporating external risk mapping
	3-2 List of material topics	pp. 18, 19, 20	Environmental Footprint, People & Culture, STEM Talent Pipeline, Data Privacy, Supply Chain, and Responsible AI
GRI 201: Economic Performance 2016	201-4 Financial assistance received from government	p. 33	Government support received in Singapore only (PWCS, CIT Rebate, NS Reimbursements)
GRI 204: Procurement Practices 2016	204-1 Proportion of spending on local suppliers	pp. 34, 35	Local procurement shares: SEA (60%), Uzbekistan (60%), Europe (50%), LATAM (50%), MEA (50%), Singapore (40%)
GRI 205: Anti-corruption 2016	205-2 Communication and training about anti-corruption	pp. 17, 33	100% completion of Code of Conduct and anti-corruption training by staff and Board
	205-3 Confirmed incidents of corruption and actions taken	pp. 33, 34	Zero confirmed incidents of corruption recorded across all operating regions

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

GRI Content index

GRI Disclosure	GRI Standard	Report Page Reference	Direct Information / Scope Notes
GRI 302: Energy 2016	302-1 Energy consumption within the organization	pp. 17, 23	Operational monitoring across core facilities; European office powered via GreenChoice renewable energy
GRI 305: Emissions 2016	305-1 Direct (Scope 1) GHG emissions	p. 23	Deemed immaterial due to leased and shared office footprint; excluded from inventory
	305-2 Energy indirect (Scope 2) GHG emissions	p. 23	161.75 tCO2eq (down 3.8% from 168.14 tCO2eq in 2024)
	305-3 Other indirect (Scope 3) GHG emissions	p. 23	4,767.22 tCO2eq (+120.1% YoY); total corporate inventory of 4,928.97 tCO2eq
GRI 308: Supplier Environmental Assessment 2016	308-1 New suppliers screened using environmental criteria	pp. 17, 34	100% of suppliers integrated into the Due Diligence Framework screening mandate
GRI 401: Employment 2016	401-1 New employee hires and employee turnover	p. 26	180 new hires (120 M / 60 F); 63 departures (41 M / 22 F) broken down by age group
GRI 403: Occupational Health and Safety 2018	403-9 Work-related injuries	pp. 25, 26	Zero work-related recordable injuries, illnesses, or fatalities
GRI 404: Training and Education 2016	404-1 Average hours of training per year per employee	p. 25	32 average hours of structured training per employee
	404-2 Programs for upgrading employee skills	pp. 26, 27, 29	LearnUpon curriculum, Soft Skills Menu, Soft Skills Camp, and technical Mentorship Program
	404-3 Employees receiving regular performance reviews	pp. 25, 26	100% of employees received structured performance and career evaluations
GRI 405: Diversity and Equal Opportunity 2016	405-1 Diversity of governance bodies and employees	pp. 25, 26, 33	Board: 5 male (100%); Leadership: 19 M / 5 F; Total Workforce: 70.1% male, 29.9% female

01 Group-IB at a Glance
02 Cybersecurity
03 ESG Strategy
04 Environment and Climate
05 Social
06 Governance
07 Appendices

GRI Content index

GRI Disclosure	GRI Standard	Report Page Reference	Direct Information / Scope Notes
GRI 413: Local Communities 2016	413-1 Operations with local community engagement	pp. 10, 14, 15, 27, 29-31	Academic Alliance across 15+ universities in 11 countries reaching 400+ students
GRI 418: Customer Privacy 2016	418-1 Substantiated complaints concerning customer privacy	pp. 33, 34	Zero substantiated customer privacy breaches and zero customer data losses
Company-Specific Disclosures: Digital Security and AI	Cybercrime disruption and law-enforcement outcomes	pp. 06, 07, 12, 13	34,838 malicious nodes disrupted; 1,809 cybercriminals arrested across 6 operations
	Responsible AI deployment and ethical safeguards	pp. 04, 08, 14, 34	Alignment with NIST AI RMF, ISO 23894, and EU AI Act; architectural human-in-the-loop oversight

Fight Against Cybercrime



GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785