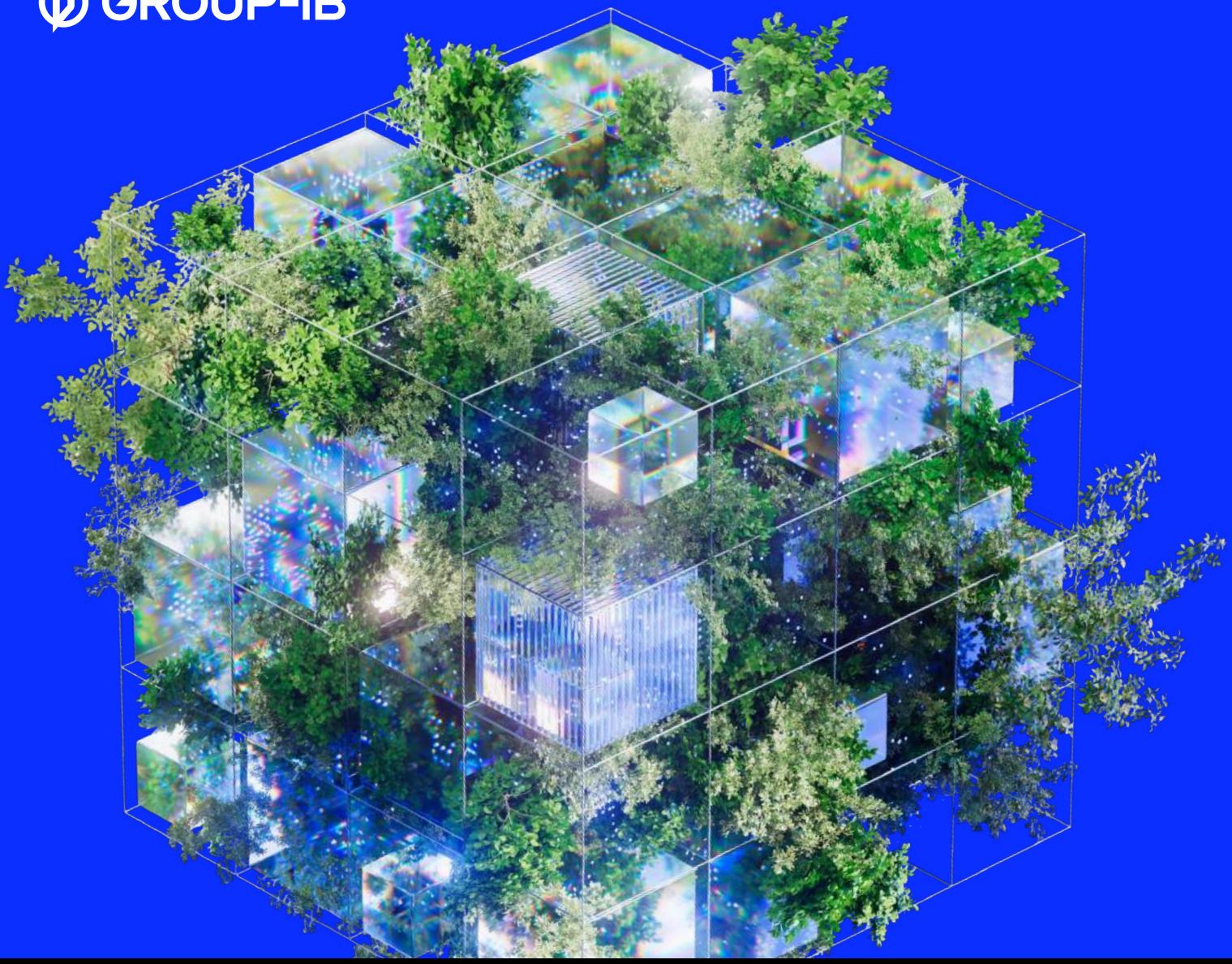
GROUP-IB



Sustainability Report 2024

Trust Through Transparency

GROUP-IB.COM

Table of Contents

About this Report

GRI 2-3

GRI 2-5

This report covers the sustainability-related strategy, policies, and performance of Group-IB Global Private Limited and its subsidiaries across key operational regions. It reflects our business approach, risk management, and ESG performance for the reporting period from 1 January to 31 December 2024. This report focuses on continuing operations and includes comparative data where relevant. Sustainability-related data may be limited for early-stage or non-operational assets due to immateriality or the progressive integration of data collection systems.

This Sustainability Report has been prepared in accordance with the Global Reporting Initiative (GRI) Standards. The report also reflects our contribution to the United Nations Sustainable Development Goals (UN SDGs).

While external assurance has not been obtained for this report, Group-IB is committed to continuous improvement in ESG reporting practices and transparency.

For any questions regarding this report, please contact: esg@group-ib.com

From the Management Team

Dmitry Volkov
CEO and Co-Founder,
Group-IB

For over two decades, Group-IB has been at the forefront of the fight against cybercrime. In pursuit of making the digital world a safer place, we have witnessed the rapid evolution of the cybersecurity landscape, marked by groundbreaking technological advancements and emerging threats. As the first private company to provide cybercrime investigation services, we have not only adapted to these changes but actively shaped them by supporting global efforts to dismantle cybercriminal networks and protect critical digital infrastructure worldwide.

Building on our tradition of innovation and research, I am proud to present Group-IB's first Sustainability Report. This milestone reflects our commitment to integrating Environmental, Social, and Governance components into every facet of our business. Our adherence to leading industry-specific standards underlines our approach to contributing to the United Nations Sustainable Development Goals. We go beyond aligning with global sustainability frameworks — we set ambitious goals to create tangible impact: combating cybercrime on a global scale while minimizing our environmental footprint, championing ethical innovation, and building a diverse, inclusive workplace.

We remain committed to deepening these practices while fostering greater accountability and transparency in our ESG efforts. This report is not just a reflection of where we stand today. It is also a testament to our dedication to building a more secure, ethical, and sustainable future for all.

Thank you for joining us on this journey.

Anastasiia Komissarova
Deputy CEO,
Group-IB

At Group-IB, we recognize that our responsibility goes beyond technological leadership. As a cybersecurity company, we are also accountable for our impact on society and the environment. Our first Sustainability Report reflects our commitment to ESG principles, which have always been embedded in our operations. With these disclosures, we aim to provide transparency to our stakeholders and reinforce the performance standards we set for the industry.

Cybersecurity is not just about defense — it is also about building a safer, more resilient digital world. We believe that the technologies we develop should protect organizations from digital threats and drive meaningful, sustainable progress. As we navigate an increasingly interconnected world, we aim to integrate security with sustainability, ensuring that innovation and responsibility are aligned. This commitment is reflected in our key initiatives:

Enhancing Inclusivity and Equal Opportunities

Fostering a workplace where every team member feels valued, empowered, and given equal opportunities to succeed in our joined mission to fight cybercrime worldwide.

Strengthening Governance

Upholding the highest standards of integrity through robust governance frameworks, clear ethics policies, and strong compliance and data protection measures.

Promoting Energy Efficiency

Enhancing energy efficiency across our offices and integrating renewable energy solutions to reduce our environmental footprint while refining our product architecture to help customers minimize their own energy consumption.

Advancing Responsible AI

Developing and deploying AI-driven technologies in an ethical way, with a strong emphasis on data privacy, security, and human rights.

Looking ahead, we remain dedicated to increasing transparency and accountability in our ESG initiatives. By continuously improving our practices and openly sharing our progress, we aim to set a benchmark for the industry and show that innovation, security, and sustainability go hand in hand and drive business forward.

Introduction

Commitment to sustainability through key approaches, data-driven insights, and strategic priorities across environmental, social, and governance pillars.

About Group-IB

Founded in 2003, Group-IB is a leading cybersecurity firm that investigates, prevents and combats digital crime. The company has built several Digital Crime Resistance Centers (DCRCs) to localize proprietary technologies, conduct local research and assist local communities in their fights against threat actors. Group-IB DCRCs are located in ten countries: Singapore, the Netherlands, the UAE, Chile, the Kingdom of Saudi Arabia, Egypt, Thailand, Malaysia, Vietnam, and Uzbekistan.

Products and Services

As part of its mission to fight against cybercrime, Group-IB offers a comprehensive suite of cybersecurity solutions, including:

Threat Intelligence
Provides insights into cyber threats to help organizations stay ahead of potential attacks.

Fraud Protection
Safeguards businesses against fraudulent activities by detecting and preventing various forms of online fraud.

Managed XDR*
Ensures real-time threat detection and response across endpoints, networks, infrastructure, and email.

Digital Risk Protection
Secures digital assets by identifying and mitigating risks across the digital environment.

Attack Surface Management
Continuously uncovers and monitors external IT assets to mitigate risks and prevent breaches.

Business Email Protection
Blocks, analyzes, and hunts for advanced email threats using patented security technology.

Group-IB also delivers a full scope of proactive and reactive services:

Group-IB Digital Forensics and Incident Response (DFIR)
We identify, contain and mitigate cyber risks by exploring the methods and motives behind intrusions, clearing infrastructure from any signs of threat, retrieving evidence to build solid cases, and monitoring networks for residual threats.

Group-IB Audit and Consulting Services
We certify, document and validate cybersecurity defenses against potential cyber risks. By addressing gaps in their existing protection measures, we help organizations manage even the most pressing business risks.

Group-IB Education and Training
We empower young professionals and corporate teams with multi-domain expertise in cybersecurity.

Hi-Tech Crime Investigations
We help organizations stop persisting cyber attacks and extract valuable insights into adversaries' tactics and infrastructure in order to identify, locate, and pursue legal action against threat actors.

[*] — Extended Detection and Response

Global Awards

Frost & Sullivan
Technology Innovation Award 2025

Singapore Police Force
Award for outstanding contribution to tackling cybercrime in Singapore 2025

CRN® Partner Program Guide 2024
Prestigious 5-Star Award for its exceptional partner program

Cybersecurity Excellence Awards 2022
Eight Gold awards including “Best Cybersecurity Company” in Asia

Top Women in Cybersecurity ASEAN 2023-2025
Honors outstanding female leaders across cybersecurity and physical security

Key Memberships

GRI 2-28

World Economic Forum — Cybercrime Atlas
Group-IB plays an active role in global initiatives to address cybercrime by sharing expertise on threat intelligence, incident response, and cyber risk management

Financial Services Information Sharing and Analysis Center
Group-IB provides insights into emerging cyber threats in its efforts to enhance sector-wide resilience and support incident response coordination

Global Anti-Scam Alliance
Group-IB is a founding member of this organization, which aims to combat scams through joint operations with global law enforcement agencies

Cybersecurity Standards

ISO/IEC committees
Contributions to ISO/IEC committees focused on information security management (ISO 27001), business continuity (ISO 22301), and risk management

Public-Private Partnerships
Involvement in public-private partnerships aimed at enhancing digital resilience in critical infrastructure sectors

Global Law Enforcement Partnerships

INTERPOL, Europol and Afripol
Providing threat intelligence, technical expertise, and investigative support to help dismantle cybercriminal networks. Our work with INTERPOL’s Cybercrime Directorate has been pivotal in global operations targeting advanced persistent threat (APT) groups and ransomware syndicates

National CERTs (Computer Emergency Response Teams)
Supporting cyber incident response and sharing knowledge with government agencies in many countries

Industry Alliances and Coalitions

Cyber Threat Alliance (CTA)
Sharing real-time threat intelligence with global cybersecurity companies to improve collective defenses against emerging threats

Forum of Incident Response and Security Teams (FIRST)
Participating in global discussions on incident response best practices and threat mitigation strategies

AI Ethics and Governance Working Groups
Engaging with multi-stakeholder initiatives focused on the responsible development and deployment of artificial intelligence technologies, ensuring alignment with human rights and data privacy standards

Academic and Research Partnerships

Cybersecurity Training Programs
Partnering with universities to develop curricula that address the evolving cyberthreat landscape

Research Collaborations
Supporting cybersecurity research projects that contribute to global knowledge on threat intelligence, digital forensics, and cybercrime investigations

Certificates and Recognition

ISO/IEC 27001:2025

ISO 9001:2025

Compliance with US DOJ

Trusted Introducer Certificate

2024 in numbers

444
employees
and 20+ languages

10
offices

500+
customers

134
patents and patent applications

60
countries served

1,221
cybercriminals arrested

~207K
instances of malicious infrastructure dismantled

~$2.7B
saved on phishing alone

~65M
victims protected (estimate)

1,291
educated individuals in cybersecurity

6
partner universities

100%
compliance with our Code of Conduct and Anti-Corruption Policies

Innovation and Digital Security

Collaboration with key stakeholders, ensuring participation in global cybersecurity alliances and fostering trusted partnerships.

Securing Digital Space through Partnership and Knowledge

Cybersecurity is an integral part of sustainability, ensuring resilience in a digital world. As a technology-driven company, we have consistently aligned our growth with the core principles of sustainability. Through our daily work in advancing the cybersecurity industry, we actively contribute to a safer digital ecosystem and help to drive sustainable development.

Recognizing the growing complexity of cyber threats, we engage in partnerships with leading global cooperation platforms, including the World Economic Forum (WEF). Group-IB has joined Cybercrime Atlas ↗, a WEF initiative designed to contribute to research into the evolving cybercrime landscape, to help dismantle cybercriminal infrastructure and operations, and to strengthen collaborations between local and international stakeholders. Group-IB analysts have already begun contributing to Cybercrime Mapping and Cybercrime Investigation Working Groups.

Cybercrime Atlas

WEF-led initiative uniting global efforts to disrupt cybercrime and enhance digital security.

> “Joining the Cybercrime Atlas initiative is not just an opportunity, it’s a responsibility. In a world where cyber threats transcend borders, collaboration is our most powerful defense. By uniting with the Cybercrime Atlas community and other key stakeholders, we connect expertise and critical intelligence, creating a united front that can disrupt criminal networks and make the digital world a safer place for everyone.
>
> 
> Dmitry Volkov
> CEO and Co-Founder

Group-IB Partner Program

Group-IB Partner Program is designed to empower businesses by offering personalized and comprehensive cyber protection solutions. By working with Group-IB, our partners can deliver exclusive cybersecurity services and technologies to their customers, ensuring robust defense against evolving digital threats.

The Program has received notable recognition, including a prestigious 5-Star Award in CRN's 2024 Partner Program Guide, underscoring its excellence and commitment to fostering strong and profitable channel partnerships.

In addition, Group-IB products have been acclaimed by industry experts. The Company was recognized as:

- Representative Vendor in 2024 Gartner Market Guide for Threat Intelligence Products & Services
- Technological Leader in “Frost Radar™: Cyber Threat Intelligence, 2024”
- Top Technology Leader in “SPARK Matrix™: Digital Threat Intelligence Management, Q2, 2024”
- Leader in “SPARK Matrix™: Digital Risk Protection (DRP), 2024”
- Challenger and Fastmover in “GigaOm 2024 Radar for Attack Surface Management”
- Representative vendor in “Emerging Tech: GenAI Security Services for Online Fraud Prevention”
- Technological Leader in “Frost Radar™: Managed Detection and Response, 2024”
- Challenger in “Kuppinger Cole: Leadership Compass Endpoint Protection Detection & Response (EPDR)”
- Leader in “SPARK Matrix™: Endpoint Protection Platforms, Q3 2024”
- Representative vendor in “2024 Gartner Market Guide for Digital Forensics and Incident Response Retainer Services”

Success Story

The effectiveness of the Group-IB Partner Program is demonstrated by collaboration with Security Lab, which improved its incident response capabilities and reduced operational costs by integrating Group-IB's Managed XDR solution, ultimately providing clients with stronger protection and an enhanced security posture.

Read the Success Story ↗

Group-IB's Research Hub ↗ serves as a central repository for comprehensive threat analyses, trend reports, blogs and white papers, providing valuable insights into the evolving cyber threat landscape.

Through initiatives such as the ones described above, Group-IB reinforces its dedication to empowering organizations and individuals with the knowledge and tools they need to navigate and mitigate the complexities of modern cyber threats.

A flagship publication is our "High-Tech Crime Trends Report 2025" ↗, which offers an in-depth examination of current and emerging cyber threats.

Group-IB's flagship report representing the latest cybercrime trends.

Key takeaways from this report include:

→ Rise in Advanced Persistent Threats (APTs)

APT-attributed attacks increased by 58% in 2024, with groups like APT28 and Gamaredon focusing on sectors such as government, energy, and military, especially in Europe.

→ Growth in Ransomware Attacks

Ransomware has evolved into a complex industry featuring Ransomware-as-a-Service (RaaS) models. In 2024, Group-IB identified 39 RaaS advertisements and a 44% rise in affiliate offers. Dedicated leak sites reported 5,066 attacks, marking a 10% increase from the previous year.

→ Increase in Phishing and Scams

Over 80,000 phishing websites were detected in 2024, 22% more than in 2023. The logistics, travel, and internet services sectors were the most targeted, accounting for 25.3%, 20.4%, and 16.4% of phishing websites, respectively. In addition, more than 200,000 fraudulent resources were identified, affecting industries such as travel, energy, financial services, logistics, and telecoms.

Computer Emergency Response Team

Group-IB's Computer Emergency Response Team (CERT-GIB) specializes in proactive cybersecurity threat detection and incident response. Operating 24/7/365, the team is dedicated to monitoring, analyzing, and mitigating cyber threats while providing expert assistance in forensic investigations and incident containment. CERT-GIB plays a critical role in safeguarding organizations from advanced cyber threats through a combination of cutting-edge technology and expertise in digital forensics, threat intelligence, and security incident management.

CERT-GIB is an active member of several prominent international cybersecurity alliances, which reinforces its capability to collaborate on global threat intelligence and incident response initiatives.

Forum of Incident Response and Security Teams (FIRST)

Anti-Phishing Working Group (APWG)

Trusted Introducer

Organization of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT)

Asia Pacific Computer Emergency and Response Team (APCERT)

By leveraging Group-IB proprietary technologies, CERT-GIB ensures a robust and proactive cybersecurity posture, enabling organizations to detect, analyze, and respond to evolving cyber threats efficiently.

Mitigating the Negative Impacts of Cybercrime

Through our proactive efforts in dismantling malicious infrastructure and preventing digital crime activities, we have directly mitigated various negative economic and environmental impacts of cybercrime, for example, from phishing attacks. Being a primary method of cybercrime, these attacks result in significant financial losses and utilize sophisticated, energy-intensive networks of computers.

22.4M kWh

energy consumption prevented by neutralizing botnets

~10K tCO_2e

emissions averted by neutralizing compromised computers

52M km

a gasoline car could travel using the energy saved from disabled botnets

~48K

decade-old trees could absorb carbon from disabled botnets

Just by neutralizing compromised computers operating under botnet control, we prevented excessive energy consumption amounting to nearly 22.4 million kWh, which equates to ~10K tCO_2e, or compared to the emissions from driving around the Earth approximately 1,297 times with 52 million kilometers in a gasoline car, or the carbon captured by ~48K tree seedlings grown for 10 years.

ESG at Group-IB

Cybersecurity as a cornerstone of sustainable development, protecting economic stability, individual privacy, and digital infrastructure.

Scope of Reporting

GRI 2-1

Group-IB headquarters is located in Singapore, but the company operates in many different countries and regions. In 2024, Group-IB conducted operations in Europe, Southeast Asia, the Middle East and Africa, Central Asia, and Latin America.

GRI 2-2

Group-IB uses different legal entities to conduct its business activities in various regions. The following list of entities has been analyzed for the purpose of sustainability reporting:

- Group-IB Global Private Limited (Singapore)
- Group-IB Europe B.V. (the Netherlands)
- Group-IB MEA FZ-LLC (the UAE)
- Group-IB SEA (Thailand)
- Group-IB TSHK (Uzbekistan)
- Group-IB Gulf (Kingdom of Saudi Arabia)
- Group-IB RHQ (Kingdom of Saudi Arabia)
- Group-IB Consultoria LATAM (Chile)

GRI 201

The Company has no financial information filed on public record. As a private company, Group-IB does not disclose financial information on revenues, costs, wages, capital payments, or investments. Such data is confidential and covered by non-disclosure agreements. However, the Company ensures financial transparency with relevant stakeholders in line with contractual and regulatory obligations.

During the reporting period, the Company did not receive any financial assistance from any government, including tax relief, subsidies, grants, awards, or financial incentives. Group-IB operates independently, without reliance on government funding.

Materiality Assessment

Company prioritizes impacts for reporting based on their significance through a materiality assessment process. The process involves:

GRI 3-1

Impact Assessment

Evaluating the scale, scope, and likelihood of each impact, with a focus on cybersecurity risks, data privacy, and operational resilience.

Stakeholder Engagement

Consulting key stakeholders, including clients, employees, and regulators, to understand their concerns, especially around data security and ethical practices.

Regulatory Compliance

Ensuring alignment with international cybersecurity standards and human rights obligations.

Alignment with Business Strategy

Prioritizing impacts that directly affect Group-IB's mission to combat cybercrime and protect digital ecosystems.

Group-IB's material topics are formed by insights from a diverse range of stakeholders and experts, including:

GRI 3-2

Clients

Key enterprise and government clients provide feedback on cybersecurity risks, data protection, and service reliability.

Employees

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

Regulators and Industry Bodies

Engagement with data protection authorities and cybersecurity regulatory bodies helps to ensure compliance with legal and ethical standards.

Business Partners

Technology vendors and strategic partners offer perspectives on supply chain security, diversity, and best practices.

Executive Leadership

The management team prioritizes topics based on strategic alignment with Group-IB's mission and long-term goals.

Material Topics

Group-IB has identified several material topics that reflect its most significant economic, environmental, and social impacts. These topics are aligned with the Company's core mission to fight against cybercrime and promote digital security, while also addressing stakeholder expectations.

GRI 3-2 GRI 3-3

Environmental Footprint

As a digital-focused company, Group-IB has a low environmental footprint, promoting energy-efficient IT practices and resource optimization in its offices.

Potential concerns, such as office energy consumption, are managed through sustainability initiatives and energy monitoring.

People and Ethics

Group-IB contributes to digital safety, data protection, and employee well-being, ensuring non-discrimination and diversity in its workforce.

Risks such as data breaches and misuse of cybersecurity tools are mitigated through strict data privacy regulations, ethical guidelines, and human rights due diligence embedded in its Code of Conduct (CoC).

Economic Performance and Business Conduct

Group-IB strengthens the global economy by reducing financial risks from cybercrime, enhancing digital trust, and supporting critical infrastructure resilience. While service disruptions and cybersecurity incidents pose potential risks, they are proactively mitigated through continuous monitoring and incident response strategies.

While Group-IB mainly partners with technology providers, suppliers, and clients, risks such as third-party data breaches or non-compliance with ethical standards are addressed through supplier assessments, stringent security policies, and adherence to its CoC.

Through continuous monitoring, compliance, and ethical business practices, Group-IB ensures that its operations and partnerships uphold high standards of cybersecurity, sustainability, and human rights protection.

Approach to Key ESG Topics

Our ESG commitments are deeply interconnected with the United Nations Sustainable Development Goals (SDGs). We actively contribute to several key SDGs through our core operations and sustainability initiatives:

SDG 9 Industry, Innovation, and Infrastructure

By enhancing global cybersecurity resilience and fostering secure digital innovation.

SDG 16 Peace, Justice, and Strong Institutions

Through combating cybercrime, supporting law enforcement, and promoting transparency.

As a growing cybersecurity company, Group-IB is at the beginning of its formal ESG journey. While we have not yet published a comprehensive ESG strategy, we recognize the importance of addressing critical topics. The areas outlined below represent our current focus and spheres of interest, which we aim to develop:

Data Privacy and Security

Given the nature of our work, we apply robust access controls, encryption, and incident response measures aligned with the GDPR and global data protection expectations to help protect client and internal information.

Responsible Business Conduct

We promote a culture of integrity and aim to manage risks through internal checks, including due diligence on partners and suppliers where appropriate.

People and Culture

We are building a team-oriented workplace and support diversity through inclusive hiring practices. Professional development is encouraged, and our employees have access to ongoing training aligned with their roles.

Environmental Awareness

As a software company, our environmental footprint is relatively low. Still, we have begun monitoring our energy use and emissions, with an interest in identifying opportunities for greater efficiency in the future.

Product Integrity and Client Trust

We incorporate secure software development practices and system monitoring as part of our service delivery, aiming to ensure the reliability and safety of our cybersecurity offerings.

Group-IB identifies actual and potential impacts through a structured risk assessment process integrated into its Quality Management System and Secure Software Engineering Guidelines.

Risk area	Mitigation measures
Cybersecurity and Data Privacy	• 24/7 CERT-GIB to detect and contain threats. • Regular security audits to identify and address vulnerabilities.
Ethical Governance and Compliance	Vetting of suppliers and partners to ensure compliance with ethical standards.
Workforce Safety and Inclusion	• Occupational health programs and secure work environment. • Diversity and equal opportunity programs to foster inclusivity.
Sustainability Efforts	• Prioritizing renewable energy sources wherever feasible. • Implementing efficient software architecture to minimize resource consumption and environmental impact.
Customer Security and Trust	• Secure Software Development Lifecycle to integrate security at every stage. • Real-time monitoring of systems to prevent cyber threats.

Group-IB uses robust processes to track how effective its actions are in managing both positive and negative impacts. The processes below ensure continuous improvement and accountability across all material topics:

Performance Monitoring

- **Key Performance Indicators (KPIs)**
  Defined for critical areas such as incident response times, data breach prevention rates, employee training completion, and energy efficiency metrics.
- **Security Metrics**
  Regular tracking of cybersecurity incidents, system vulnerabilities, and threat mitigation effectiveness through advanced monitoring tools.

Internal and External Audits

- **Regular Audits**
  Conducting internal audits aligned with ISO 27001 and ISO 9001 standards and periodic external assessments to verify compliance with security, ethical, and sustainability standards.
- **Compliance Reviews**
  Ongoing reviews of adherence to data protection laws, such as GDPR, and internal policies.

Continuous Improvement Framework

- **Incident Post-Mortems**
  Root cause analyses and lessons learned from security incidents or policy breaches to refine practices and prevent recurrence.
- **Feedback Loops**
  Collecting feedback from clients, employees, and stakeholders to assess the real-world impact of Group-IB's actions.

Reporting and Transparency

- **Management Reviews**
  Regular reporting to senior leadership on the performance of sustainability initiatives and security measures.
- **Stakeholder Engagement**
  Transparent communication with stakeholders through sustainability reports, client updates, and regulatory disclosures.

Certification and Benchmarking

- **Industry Certifications**
  Maintaining and renewing relevant cybersecurity certifications to benchmark effectiveness against global best practices.
- **Benchmarking**
  Comparing performance with industry peers to identify gaps and opportunities for improvement.

Sustainability Targets

Qualitative and quantitative targets to drive meaningful, measurable and accountable impact on E, S and G pillars.

Committed to a Sustainable and Transparent Digital Future

As a cybersecurity company dedicated to digital resilience and environmental responsibility, we have established clear, qualitative and quantitative ESG targets to steer our efforts toward meaningful impact.

In 2024, we started to measure our Scope 1, 2 and 3 GHG emissions, laying the groundwork for transparent reporting. Furthermore, we are proud to report that since 2025, our EU office operates entirely on green energy sources, demonstrating our commitment to the clean energy transition and climate responsibility.

While we continue working toward minimizing our environmental impact, our near-term objectives emphasize advancing inclusive social programs and strengthening governance. Our efforts reflect our conviction that cybersecurity and sustainability are deeply interconnected.

Social	Governance
Provide internal training programs focused on ethics and sustainability to >90% employees. Deadline: 2026	Develop and publish an ESG program and materiality matrix. Deadline: 2026
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	Embed ESG principles into procurement through a supplier Code of Conduct and Due Diligence Framework, screen 100% of suppliers. Deadline: 2026

Approach to Stakeholder Engagement

Collaborative and inclusive approach to stakeholder engagement, ensuring alignment with the mission and supporting long-term sustainable growth.

Stakeholder Engagement

The Company adopts a strategic and inclusive approach to stakeholder engagement, ensuring that interactions align with its mission, drive collaboration, and foster sustainable growth.

GRI 2-29

Group-IB maintains continuous engagement with key stakeholders which plays a critical role in shaping its actions:

Stakeholder Group	Engagement Topic	Engagement Type	Measurement
Citizens and Society	Cyber threat protection and awareness	• Awareness campaigns • Educational programs	• Number of awareness events • Reach metrics
Law Enforcement	Cybercrime investigation support	• Collaborative partnerships • Threat intelligence sharing	• Number of joint operations • Shared intelligence cases
Corporate Clients and Partners	Cybersecurity service reliability and innovation	• Regular consultations • Feedback mechanisms	• Customer satisfaction scores • Service feedback
Academia	Cyber education and talent development	• Research partnerships • Curriculum development	• Number of academic partnerships • Number of program participants
Shareholders and Employees	Company growth and workplace environment	• Surveys • Internal communications • Training initiatives	• Employee engagement survey results • Retention rates
Regulatory Bodies	Data protection and compliance	• Policy dialogues • Compliance reviews	• Compliance audit outcomes • Policy updates
Technology Partners and Suppliers	Supply chain security and compliance	• Joint risk assessments • Ethical standards alignment	• Third-party risk assessments • Supplier compliance rate

Environment and Climate

Prioritizing energy efficiency, emissions monitoring and responsible resource consumption across our operations.

Building Cyber Resilience with Environmental Responsibility

The global IT industry is responsible for an estimated 2–4% of worldwide greenhouse gas (GHG) emissions, a figure comparable to the aviation sector and projected to rise as digital demand grows. In 2024, Group-IB established a baseline for measuring our carbon footprint. Since then, we have been committed to transparently reporting our performance indicators.

As an information technology company, we understand that our environmental impact may not be as apparent as in other industries. However, we acknowledge that our operations powered by AI, data centers, and digital infrastructure rely on the Planet's resources, especially energy.

Our Approach

We take a comprehensive approach to embedding environmental awareness across our organization. Doing so includes:

Measuring our emissions

In accordance with the globally recognized Greenhouse Gas Protocol (GHG Protocol).

Reducing our environmental impact

Through conscious operational choices, such as partnering with green energy providers, minimizing waste, promoting recycling and optimizing product architecture.

Internal policies and educational initiatives

Implementing internal policies and educational initiatives that encourage sustainable practices across all levels of the company.

Guidelines and Accounting Approach

GHG Protocol

Corporate Accounting and Reporting Standard for energy and emissions calculations.

GRI Standards

Guidelines for energy consumption and emissions reporting.

Official Databases

Energy conversion factors are sourced from official databases (e.g., EEA, BEIS, EXIOBASE and World Bank).

Scope 2 Emissions

For Scope 2 emissions, both location-based and market-based approaches are considered as applicable.

Energy Consumption and Emissions

GRI 302

During the reporting period, Group-IB did not consume any energy outside its operational boundaries. Due to the nature of the business as a software company, energy use is limited to internal operations, including office facilities, data centers, and employee workspaces. The Company does not engage in energy-intensive activities such as manufacturing, logistics, or outsourced production that would result in significant energy consumption beyond its direct control. As a result, there is no recorded energy consumption outside the organization's operational scope. All energy consumed is used solely for internal operations, and no surplus energy is supplied to external parties or the grid.

376,605 kWh

Total Electricity Consumption

71,024 kWh

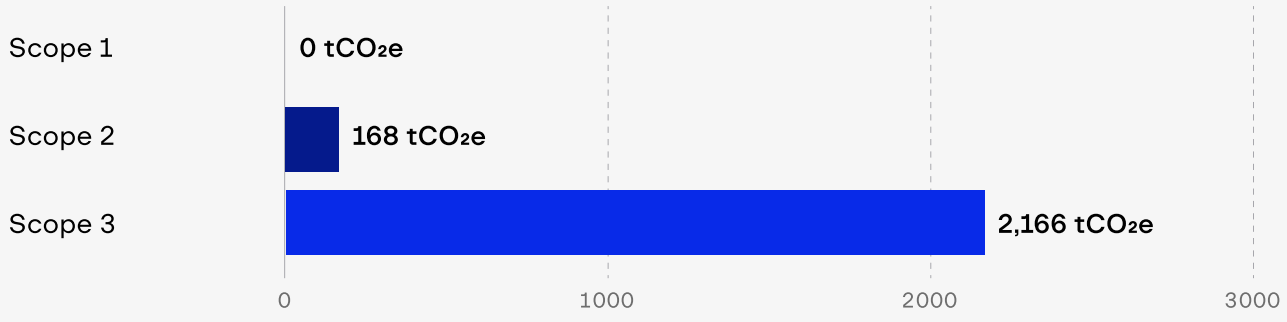
Total Heating Consumption

GRI 305

Group-IB does not produce Scope 1 emissions as its activities as a cybersecurity firm do not involve direct fuel combustion, industrial operations, or company-owned vehicles. No direct greenhouse gases are therefore emitted from sources under its ownership or control. The Company's focus on digital and cloud-based services further contributes to its minimal direct environmental impact.

In 2024, Group-IB reported 168 tCO_2e of Scope 2 GHG emissions and 2,166 tCO_2e of Scope 3 emissions, with 1,541 tCO_2e attributed to Purchased Goods and Services and 625 tCO_2e to Business Travel.

Group-IB Carbon Emissions in 2024



Shared Responsibility: Green Energy in Our Dutch Office

As part of our efforts to operate more sustainably, Group-IB partnered with Greenchoice in 2024 to supply our Dutch office, home to 27 employees, with 100% renewable electricity sourced from wind and solar energy. This collaboration reflects our commitment to minimizing our operational footprint, even as a digitally focused company.

Greenchoice is not only a renewable energy provider. It also plays an active role in global climate action through investments in biodiversity restoration, including mangrove reforestation projects in Guinea-Bissau. These initiatives contribute to natural CO_2 absorption and the protection of fragile ecosystems.

While our environmental impact is relatively modest, choosing clean energy providers like Greenchoice allows us to align our daily operations with broader global decarbonization efforts, reinforcing our belief that sustainability is a shared responsibility, even for small offices in the digital sector.

Since 2024, electricity for the Dutch office is 100% renewable
Image courtesy of Group-IB

Greenchoice invests in biodiversity, including mangrove reforestation projects in Guinea-Bissau
Image source: Greenchoice | Samen impact maken door mangroven van Guinee-Bissau te herstellen ↗

Social

Empowering people through diversity, inclusion, and continuous development in the fight against cyber threats.

Human Capital at the Core of Cyber Defense

At the heart of our business lies an in-depth understanding that people are our most powerful asset. As a cybersecurity company operating in a knowledge-driven industry, Group-IB depends on cultivating an inclusive, resilient, and empowered workforce. From competitive and equitable compensation to well-being initiatives and professional growth, we are committed to creating a work environment where our people can develop and receive the support they need. We demonstrate our commitment through the following initiatives:

Diverse and Global Team

The Company maintains a strong focus on having a diverse team with experts from over 30 countries and has introduced policies that support diversity and inclusion in the workplace.

Our Global Team is from

30 countries

Career Development

Group-IB ensures opportunities for career progression, with several policies in place that encourage internal mobility and professional growth.

Internship Program

The Company offers internships aimed at building careers in cybersecurity. The initiative shows our commitment to nurturing young talent and providing growth opportunities within the company.

> Cybersecurity thrives on diverse minds tackling complex challenges. At Group-IB, talent is measured by expertise and impact, not gender. Equality isn't just a goal. It's our standard.

Anastasia Tikhonova
Technical Head, The Unified Risk Platform, APAC

> Group-IB helped me navigate uncharted territories and gain a whole new level of expertise in cybersecurity. My journey started from Singapore, and then an exciting opportunity brought me to Riyadh. Adding to the thrill was a shift in my product focus. The product knowledge gaps and cultural nuances seemed overwhelming at first, but the incredible support from my colleagues made it easy. They didn't just inspire me to succeed, but to also help others on similar paths.

Alfian Bin Sujak
Implementation Engineer

Our Employees

Employment Practices

GRI 401

During the reporting period, the Company onboarded 183 new employees and recorded the departure of 50 employees across its various operational locations. The Company also works with a number of independent contractors, mainly in Europe and Singapore. All employees across all regions are entitled to parental leave in accordance with local labor laws and company policies. Health insurance is provided to full-time employees across all locations, and the Company continuously reviews its benefits program to support employee well-being and industry best practices.

GRI 202

GRI 402

Group-IB ensures gender-equal and competitive entry-level wages across all locations, consistently exceeding local minimum wage standards. Compensation for independent contractors is reviewed to align with market benchmarks and labor laws, reinforcing the Company's commitment to equitable and competitive pay across all regions. The Company provides a 3 to 4-week notice period for significant operational changes, ensuring transparency and alignment with best employment practices.

The Company employs senior management across its locations of operation, with a focus on global expertise. While most senior management is internationally sourced, the Company strives to recruit local talent for leadership positions.

Occupational Health and Safety

GRI 403

As an office-based cybersecurity company with minimal workplace risks, Group-IB does not maintain formal occupational health services or an occupational health and safety management system.

However, employee well-being is prioritized through ergonomic workspaces, first aid availability, emergency response protocols, and health insurance, including dental and mental well-being support. During onboarding employees receive occupational health and safety training that covers office safety, emergency procedures, and ergonomic best practices.

No work-related injuries or cases of work-related ill health were recorded during the reporting period, with the primary workplace risk being prolonged postural immobility. To mitigate this, the Company promotes an active lifestyle through initiatives such as semi-annual sports competitions. While no formal audits or joint safety committees exist, employees are encouraged to communicate workplace safety concerns to HR, which helps to foster a safe and comfortable work environment.

Ethics

GRI 405

GRI 406

GRI 407

The Company ensures diversity within its governance bodies and employee categories by analyzing representation based on gender, age group, and minority status across all locations of operation. It maintains a gender-equal pay structure and equal basic salary and remuneration for men and women across all employee categories. No incidents of discrimination requiring reviews, remediation, or corrective action were recorded during the reporting period.

The Company has no operations or suppliers where workers' rights to freedom of association and collective bargaining are at significant risk. As an office-based organization, it does not operate in high-risk industries or regions with labor rights restrictions.

In addition, the Company has no operations or suppliers at significant risk for child labor or forced labor. Group-IB upholds strict due diligence and compliance policies to ensure that all business relationships adhere to ethical labor standards, thereby contributing to the prevention of child and forced labor.

GRI 408

GRI 409

The Company's employees are not covered by collective bargaining agreements except in the case of interns in Singapore, where it is legally required. Employment terms are determined through internal HR policies, market benchmarks, and local labor laws, ensuring fair, transparent, and competitive working conditions without reliance on external agreements.

GRI 2-30

Training and Performance Review

During the reporting period, employees received 32 hours of training on average across all geographic locations and roles. While the Company does not currently offer formal upskilling or transition assistance programs, employees are encouraged to pursue self-directed learning and professional development. Furthermore, all employees received performance and career development reviews, ensuring continuous feedback and growth opportunities.

GRI 404

100%

of employees received performance and career development reviews

32

hours of training on average per year

Education and Research

Group-IB is committed to advancing cybersecurity through continuous research, education, and knowledge sharing. We actively collaborate with leading universities worldwide, fostering the next generation of cybersecurity experts.

Our commitment extends to building specialized training courses for university professors that allow them to level-up their knowledge and thus provide the most relevant and practical education to their students as well as building Group-IB-powered SOC centers where students can practice their newly gained knowledge.

Group-IB also strives to develop accessible online knowledge databases featuring expert-led webinars, industry-specific research, and white papers that provide critical insights into emerging threats.

By prioritizing education and research, we not only raise awareness, but also empower organizations and individuals to prevent cyber threats and contribute to a safer digital world.

1291

number of individuals trained

6

partnerships with universities

To further its educational mission, Group-IB created a Knowledge Hub ↗ that explains and demystifies fundamental cybersecurity concepts, such as the role of Blue Teams, methodologies for assessing cyber risks, and tools for understanding botnets. Group-IB also shares expert knowledge of basic cybersecurity through a special series of videos on YouTube ↗ as well as insights into the most notorious threat actors through its podcast called Masked Actors ↗, available on podcast platforms. To complement these resources, Group-IB hosts a series of webinars designed to equip organizations with actionable intelligence and strategies that will enhance their security posture.

Fraud Matrix 1.5 Webinar: New Features You Need to Know

This session unveils the latest advancements in Group-IB's fraud prevention tool, offering insights into enhanced mitigation strategies and streamlined detection methods.

Get the Webinar ↗

Beyond the Traditional SOC: Intelligence-Driven Security Operations

This webinar explores how to transform Security Operations Centers through intelligence-driven strategies, addressing current challenges and demonstrating how integrated threat intelligence improves incident monitoring, response, and threat hunting.

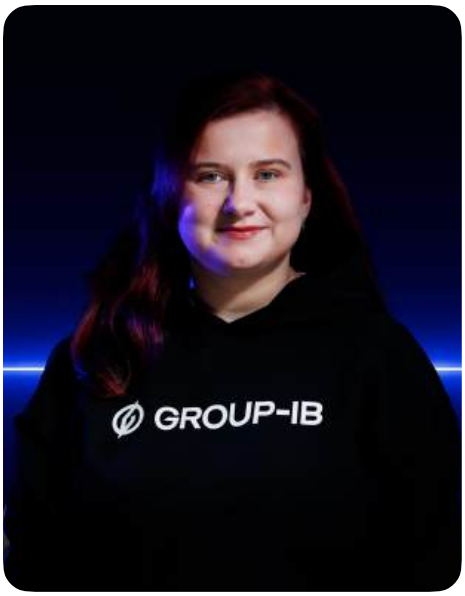
Get the Webinar ↗

Breaking Barriers in Cybersecurity

At Group-IB, we are proud to support female leadership and empower women in cybersecurity. Our commitment to gender diversity is reflected, among other things, in the remarkable achievements of Anastasia Tikhonova, Jennifer Soh, and Vesta Matveeva, who were named among the Top 30 Women in Security ASEAN Region ↗, several years in a row. The prestigious recognition underscores their expertise and our dedication to creating an inclusive environment where all talent thrives.

> We don't just open doors for women in tech — we ensure they have a seat at the table, that their voices are heard, and that they receive the recognition they deserve. The same commitment extends to all underrepresented groups, because true innovation thrives in a rich plethora of diverse minds, perspectives, and talents.
>
> 
> Anastasiia Komissarova
> Deputy CEO

Top Women in Security ASEAN Awards 2024



Anastasia Tikhonova
Technical Head,
The Unified Risk Platform,
APAC

Jennifer Soh
Cyber Investigation Lead,
APAC

Vesta Matveeva
Head of High-Tech Crime
Investigation Department,
APAC

Governance

Strong governance underpins our role as a reliable cybersecurity partner, driving ethical conduct, transparency, and sustainable business practices.

Transparent Governance in a Connected World

Our governance framework is designed to uphold the highest standards of operational excellence, accountability, and strategic oversight. The Board of Directors, comprising both executive and independent members, guides the organization with a clear focus on risk management, ethical conduct, and long-term value creation.

As we present our inaugural Sustainability Report, we do so with the same precision and responsibility that define our approach to cybersecurity — one anchored in trust, guided by ethics, and driven by leadership that prioritizes stakeholder alignment and positive impact.

Our Board of Directors

GRI 2-9

The Company's governance structure is designed to ensure strategic oversight, accountability, and effective decision-making. The Board of Directors serves as the highest governance body, with each shareholder represented on the Board.

The Board holds quarterly meetings to review progress on key strategic initiatives, while the Annual Board Meeting focuses on approving the budget and setting development priorities for the upcoming year.

The Board comprises five members, both executive and non-executive, ensuring a balanced mix of dependent and independent perspectives. Although the current composition is entirely male, the Company is committed to enhancing diversity and promoting inclusive representation in future appointments.

In addition, the governance structure ensures that key stakeholders, including shareholders, employees, and strategic partners, are represented, with the recent appointment of Mr. Craig Jones as a Strategic Advisor, which further strengthens our engagement with law enforcement and governance stakeholders.

> Collaboration between law enforcement agencies and private cybersecurity companies is essential in the fight against cybercrime. Group-IB has long been a trusted partner to global law enforcement, and since joining as an independent advisor, I remain committed to strengthening these partnerships, fostering transparency, and building trust. In an ever-evolving threat landscape, integrity and cooperation are our most valuable assets.
>
> 
>
> Craig Jones
> Independent Strategic Advisor

GRI 2-10

The Board nomination and selection process is designed to ensure that highly qualified individuals are appointed to oversee strategy, governance, and risk management. Shareholders can nominate candidates, who must pass a rigorous security clearance to uphold the Company's cybersecurity standards.

The selection criteria for Board members prioritize stakeholder input, with shareholder nominations complemented by insights from business partners and senior management to align candidates with the Company's strategic goals. The criteria also emphasize maintaining a balanced mix of executive and independent members to ensure objective judgment and avoid conflicts of interest. In addition, candidates are expected to demonstrate expertise in cybersecurity, financial governance, strategy, and regulatory compliance, supporting the Company's overall impact on the economy, the environment, and society.

GRI 2-12

The Board steers the Company's strategy, governance, and sustainability, with key decisions requiring formal approval under the Shareholders' Agreement. It sets and regularly updates the Company's mission, values, and strategies to align with sustainability goals, while senior executives implement these strategies and report on progress. The Board is responsible for reviewing and approving the Company's sustainability information and managing material topics, ensuring that sustainability is integrated into its strategic priorities. The Board works with senior executives to identify key economic, environmental, and social issues through stakeholder engagement and risk assessments.

GRI 2-14

The Board reviews regular updates and draft reports from the Global CEO and management, approving disclosures that meet global standards such as the GRI. Continuous feedback is provided to improve reporting quality, reinforcing the Company's commitment to responsible, transparent, and resilient long-term growth. The Board also engages stakeholders to inform risk and opportunity assessments and reviews due diligence findings related to cybersecurity, privacy, and sustainability. Quarterly governance and risk management reviews, together with an annual in-depth assessment, help to ensure continuous improvement.

GRI 2-11

The Global CEO also serves as the Chair of the Board, merging executive leadership with board oversight to advance strategy, growth, and governance in cybersecurity. In an industry marked by rapid growth and high risk, deep cybersecurity expertise, and the profound understanding of the Company's operations and cyber threats uniquely qualifies him for this role.

GRI 2-13

To maintain transparency, the Global CEO provides monthly updates to key Board members on strategic progress, holds quarterly all-staff meetings to share organization-wide updates, and conducts an annual comprehensive review to ensure that Group-IB's strategy aligns with impact goals.

The Global CEO assigns senior executives who lead strategic initiatives across economic, environmental, and social areas, while key employees across departments are responsible for embedding sustainability and compliance throughout the organization.

“

Strong corporate governance isn’t just a framework — it’s the foundation of trust, transparency, and sustainable success. A diverse and strategic Board of Directors ensures we make decisions that drive long-term value, uphold integrity, and navigate the future with confidence.

Dmitry Volkov
CEO and Co-Founder

Code of Conduct and Compliance

GRI 2-15

Group-IB upholds integrity and transparency by proactively preventing, identifying, and managing conflicts of interest among all stakeholders. All employees undergo rigorous security clearance, including polygraph tests, while regular due diligence on contractors, partners, and customers mitigates risks.

Our strict Code of Conduct requires employees and Board members to disclose financial interests, relationships, and affiliations. The Board reviews all such disclosures and enforcing recusal procedures as needed.

Transparency is also ensured by disclosing cross-board memberships, shareholding details, controlling shareholder influences, and related-party transactions in financial statements, which collectively reinforces ethical governance and stakeholder trust.

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

GRI 2-16

Group-IB has created an open communication channel that allows critical issues to be escalated to the Board immediately. At any time, the Global CEO or any top-level manager can contact the Board directly — outside of scheduled meetings to report serious concerns, including significant cybersecurity breaches, compliance or legal risks, financial irregularities, operational challenges, reputational or ethical issues, and matters affecting sustainability and stakeholder trust. Such a flexible process ensures that the Board is continuously informed and able to act swiftly to safeguard the Company's operations and reputation. During the reporting period, the Company did not identify or communicate any critical concerns to the highest governance body.

GRI 2-17

The Company bolsters the Board's sustainability expertise through regular training and workshops on ESG, climate risks, and ethical governance led by external experts. Board members also engage in cross-sector sustainability forums for industry benchmarking and are encouraged to pursue executive education in sustainable leadership to ensure continuous learning.

GRI 2-18

Group-IB conducts annual evaluations to enhance governance and sustainability. These evaluations include annual reviews that assess strategic oversight, risk management, and ESG integration based on criteria such as effectiveness in sustainability, stakeholder engagement, and risk management. Board members also engage in self and peer reviews to evaluate both individual and collective performance.

Alignment with Global Standards

Group-IB demonstrates strong alignment with global cybersecurity standards by maintaining international certifications, collaborating with law enforcement agencies, and adhering to strict data protection and threat intelligence protocols.

GRI 2-23

Audited as partner of **INTERPOL**	Audited as partner of **EUROPOL**	Audited as partner of **AFRIPOL**
Certified **ISO 9001**	Certified **ISO/IEC 27001**	
Independently assessed for compliance **U.S. Department of Justice**	Operates in accordance with **EU General Data Protection Regulation (GDPR)**	

Due Diligence and Risk Management

- Assesses ethical, legal, and sustainability risks.
- Conducts compliance checks and continuous monitoring.
- Applies a precautionary approach to cybersecurity, privacy, and human rights.

Human Rights Commitment

- Supports privacy, fair labor, and protection from exploitation.
- Prioritizes vulnerable groups, including whistleblowers and victims of cybercrime.

Policy Access and Governance

- Available to employees and provided upon request to individuals outside the company.
- Approved and reviewed by the Board.

Application and Communication

- Applies to all operations, suppliers, and partners.
- Communicated via training, onboarding, and contractual clauses.

The Head of Security manages conflicts of interest, clearances, and compliance with sanctions. The Head of Compliance oversees IT security and cybersecurity policies. The Head of Threat Intelligence ensures ethical threat research. All these responsibilities are embedded in corporate strategy, policies, and standard operating procedures, ensuring consistent ethical practices across operations.

During the reporting period, the Company recorded zero significant instances of non-compliance, which also means that it incurred no monetary or non-monetary sanctions.

GRI 2-27

100%

anti-corruption policies acknowledgement

100%

operations assessed for risks

0

significant instances of non-compliance

Regular internal audits, compliance reviews, and risk assessments ensure adherence to regulations. Group IB's commitment to ethical practices and strong internal controls has made it possible to maintain a full compliance record.

Anti-Corruption and Fair Competition

GRI 205

During the reporting period, Group-IB recorded no confirmed incidents of corruption and had no pending or completed legal actions related to anti-competitive behavior, anti-trust, or monopoly violations.

With its zero-tolerance policy on corruption, the Company conducts comprehensive risk assessments across all of its operations and enforces strict internal controls, due diligence, and compliance monitoring to ensure adherence to ethical standards and anti-corruption laws.

Group-IB proactively communicates its anti-corruption policies and procedures to all relevant stakeholders and mandates training for employees and governance body members. Similarly, the Company remains committed to fair competition, ensuring full compliance with anti-trust and monopoly regulations across all jurisdictions.

Supply Chain and Product Safety

Group-IB operates in the fields of information security, IT, software development, IT consulting, and educational services.

GRI 2-6

Its supply chain is streamlined, with 100% of software development conducted in-house, regional data hosting ensured by providers like Hetzner and AWS, and third-party providers handling marketing, legal, and financial services worldwide.

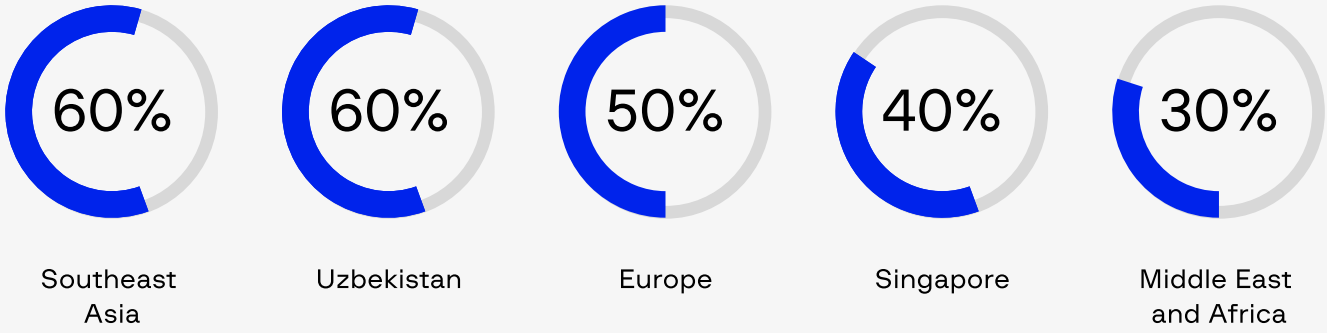
100%
of software development conducted in-house

Following a 3-tier model, the Company distributes software through partners and distributors, who also manage logistics and hardware procurement when necessary.

We are committed to supporting local economies by engaging with local suppliers across all locations of operation.

GRI 204

Proportion of spending on local suppliers



Group-IB does not have formal requirements for product and service information labeling, as its offerings do not require physical labeling or environmental disclosures.

GRI 417

100%
products and services assessed for health and safety

The Company reported no incidents of non-compliance related to product labeling, service information, or marketing communications during the reporting period and ensured adherence to all applicable legal and ethical standards.

During the reporting period, the Company recorded no breaches of customer privacy or data security incidents, maintaining strict data protection measures.

GRI 416

All of significant product and service categories were assessed for health and safety impacts, with no incidents of non-compliance identified.

Contact Information

Singapore

Address	068900, Singapore, 108 Robinson Road, #07-01
24/7 Incident Response Team	+65 3159-4398
General Inquiries	+65 3159-3798

Netherlands

Address	1017KD, Amsterdam, Prinsengracht 919
24/7 Incident Response Team	+31 20 890 55 59
General Inquiries	+31 20 226 90-90

Chile

Address	Av. Presidente Riesco 5435, Oficina 202, Las Condes, Región Metropolitana, Chile, 7561127
24/7 Incident Response Team	+65 3159-4398
General Inquiries	+65 3159-3798

United Arab Emirates

Address	Dubai Internet City, Building @3, Office 102, Dubai, UAE
24/7 Incident Response Team	+971 4 540 6400
General Inquiries	+971 4 568 1785

Malaysia

Address	C4-2-6, Solaris Dutamas, 1 Jalan Dutamas 1, 50480, Kuala Lumpur
24/7 Incident Response Team	+65 3159-4398
General Inquiries	+6017-5191099

Uzbekistan

Address	Abdulla Qodiriy Street 1A, 6th floor, Tashkent, Uzbekistan
24/7 Incident Response Team	+65 3159-4398
General Inquiries	+65 3159-3798

Vietnam

Address	117200, Hanoi, 16th floor, TNR Tower, 54A Nguyen Chi Thanh, Lang Thuong Ward, Dong Da District, Hanoi, Vietnam
24/7 Incident Response Team	+65 3159-4398
General Inquiries	+84 24 4458 3354

Thailand

Address	77, 77 Chalermprakiat Ratchakan Thi 9 Road, Ratsada, Mueang Phuket District, Phuket 83000, Thailand
24/7 Incident Response Team	+65 3159-4398

Appendix 01

Sustainability Performance Table

Environmental Data

Scope 1	Scope 2	Scope 3	Electricity consumption	Total Heating Consumption
0 tCO_2e	168 tCO_2e	2,166 tCO_2e	376,605 kWh	71,024 kWh

Social and Governance

Total Workforce Summary

Total Male Employees	Total Female Employees	Total Employees
339	105	444

Total Employees by Region and Gender

Region	Male	Female	Total
EU	24	3	27
MEA	45	16	61
SEA	34	9	43
SG	178	39	217
UZ	59	37	96

Hires Under 30 Years Old

Region	Male	Female	Total
EU	1	2	3
MEA	5	5	10
SEA	1	3	4
SG	16	8	24
UZ	22	23	45

Hires Aged 30-50 Years Old

Region	Male	Female	Total
EU	1	1	2
MEA	19	3	22
SEA	7	0	7
SG	43	6	49
UZ	12	5	17

Hires Aged 50+ Years Old

Region	Male	Female	Total
SG	0	1	1

Total New Employee Hires

Under 30	30–50	50+	Total Hires
85	97	1	183

Europe (EU), Middle East & Africa (MEA), Southeast Asia (SEA), Singapore (SG), Uzbekistan (UZ)

Turnover Under 30 Years Old

Region	Male	Female	Total
EU	0	0	0
MEA	0	0	0
SEA	1	0	1
SG	4	4	8
UZ	10	1	11

Turnover Aged 30-50 Years Old

Region	Male	Female	Total
EU	1	0	1
MEA	1	2	3
SEA	2	1	3
SG	14	3	17
UZ	3	3	6

Total Employee Turnover

Under 30	30–50	Total Employee Turnover
20	30	50

Parental Leave

Age Group	Region	Employees on Parental Leave
30–50 years	MEA	1

Diversity Among Employees by Gender and Age Group

Under 30	30–50	Over 50 years
Significant presence, especially in technical and operational roles	Majority of employees, particularly in management and leadership positions	Limited presence, primarily in governance roles

Training and Education

Average hours of training per year per employee	Percentage of employees receiving regular performance and career development reviews
32	100%

Security Practices

Security personnel trained in human right policies or procedures
100%

Proportion of Spending on Local Suppliers

EU	MEA	SEA	SG	UZ
50%	30%	60%	40%	60%

Europe (EU), Middle East & Africa (MEA), Southeast Asia (SEA), Singapore (SG), Uzbekistan (UZ)

Governance Body Diversity by Gender and Age Group

Region	Male	Female	Age <30	Age 30–50	Age >50	Minority Representation
EU	2	0	0	0	0	No
MEA	12	4	0	15	1	No
SEA	2	1	0	3	0	Yes
SG	5	2	0	7	0	Yes
UZ	1	0	1	0	0	No

Compliance with Laws and Regulations and Anti-Corruption

Significant instances of non-compliance	0
Confirmed incidents of corruption	0
Operations assessed for risks related to corruption	100%
Legal actions for anti-competitive behavior, antitrust, and monopoly practices	0

Communication of Anti-Corruption Policies

Percentage of Governance Body Members received and acknowledged the Company's anti-corruption policies across all regions	100%
Percentage of employees across all categories and regions have been informed about anti-corruption policies as part of their onboarding process and ongoing compliance updates	100%
Percentage of business partners informed about the Company's anti-corruption policies, ensuring adherence to ethical standards	100%

Anti-Corruption Training

Percentage of Governance Body Members that have completed anti-corruption training	100%
Percentage of employees across all regions and categories receive mandatory anti-corruption training during onboarding and periodic refresher courses	100%

Europe (EU), Middle East & Africa (MEA), Southeast Asia (SEA), Singapore (SG), Uzbekistan (UZ)

Customer Health and Safety	
Assessment of the health and safety impacts of product and service categories	Incidents of non-compliance concerning the health and safety impacts of products and services
100% of significant product and service categories	0

Customer Privacy
Substantiated complaints concerning breaches of customer privacy and losses of customer data
0

Appendix 02

GRI Content Index

General Disclosures

GRI Standard	Disclosure	Location
GRI 2 General Disclosures 2021	2-1 Organizational details	p.17
	2-2 Entities included in the organization's sustainability reporting	p.17
	2-3 Reporting period, frequency and contact point	p.02
	2-5 External assurance	p.02
	2-6 Activities, value chain and other business relationships	p. 46
	2-7 Employees	p. 50
	2-9 Governance structure and composition	p. 39
	2-10 Nomination and selection of the highest governance body	p. 39
	2-11 Chair of the highest governance body	p.40
	2-12 Role of the highest governance body in overseeing the management of impacts	p.40
	2-13 Delegation of responsibility for managing impacts	p.40

Continuation of the Table

GRI Standard	Disclosure	Location
GRI 2 General Disclosures 2021	2-14 Role of the highest governance body in sustainability reporting	p. 40
	2-15 Conflicts of interest	p. 42
	2-16 Communication of critical concerns	p. 42
	2-17 Collective knowledge of the highest governance body	p. 42
	2-18 Evaluation of the performance of the highest governance body	p. 42
	2-22 Statement on sustainable development strategy	p. 21
	2-23 Policy commitments	p. 43
	2-24 Embedding policy commitments	p. 21
	2-27 Compliance with laws and regulations	p. 44
	2-28 Membership associations	p. 07
	2-29 Approach to stakeholder engagement	p. 27
	2-30 Collective bargaining agreements	p. 35

Material Topics

GRI Standard	Disclosure	Location
GRI 3 Material Topics 2021	3-1 Process to determine material topics	p.18
	3-2 List of material topics	p.18
	3-3 Management of material topics	p.20
GRI 201 Economic Performance 2016	201-4 Financial assistance received from government	p. 17
GRI 202 Market Presence 2016	202-1 Ratios of standard entry level wage by gender compared to local minimum wage	p.34
	202-2 Proportion of senior management hired from the local community	p.34
GRI 204 Procurement Practices 2016	204-1 Proportion of spending on local suppliers	p. 46
GRI 205 Anti-corruption 2016	205-1 Operations assessed for risks related to corruption	p. 52
	205-1 Communication and training about anti-corruption policies and procedures	p. 52
	202-2 Confirmed incidents of corruption and actions taken	p. 52

GRI Standard	Disclosure	Location
GRI 302 Energy 2016	302-1 Energy consumption within the organization	p. 30
	302-2 Energy consumption outside of the organization	p. 30
GRI 305 Emissions 2016	305-1 Direct (Scope 1) GHG emissions	p. 30
	305-2 Energy indirect (Scope 2) GHG emissions	p. 30
	305-3 Other indirect (Scope 3) GHG emissions	p.30
GRI 401 Employment 2016	401-1 New employee hires and employee turnover	p. 50
	401-3 Parental leave	p.51
GRI 402 Labor / Management Relations 2016	402-1 Minimum notice periods regarding operational changes	p. 34

GRI Standard	Disclosure	Location
GRI 403 Occupational Health and Safety 2018	403-1 Occupational health and safety management system	p.34
	403-2 Hazard identification, risk assessment, and incident investigation	p. 34
	403-3 Occupational health services	p. 34
	403-4 Worker participation, consultation, and communication on occupational health and safety	p. 34
	403-6 Promotion of worker health	p. 34
GRI 404 Training and Education 2016	404-1 Average hours of training per year per employee	p. 35
	404-2 Programs for upgrading employee skills and transition assistance programs	p. 35
	404-3 Percentage of employees receiving regular performance and career development reviews	p. 35
GRI 405 Diversity and Equal Opportunity 2016	405-1 Diversity of governance bodies and employees	p. 34
	405-2 Ratio of basic salary and remuneration of women to men	p.34

GRI Standard	Disclosure	Location
GRI 406 Non-discrimination 2016	406-1 Incidents of discrimination and corrective actions taken	p.34
GRI 407 Freedom of Association and Collective Bargaining 2016	407-1 Operations and suppliers in which the right to freedom of association and collective bargaining may be at risk	p.34
GRI 408 Child Labor 2016	408-1 Operations and suppliers at significant risk for incidents of child labor	p.35
GRI 409 Forced or Compulsory Labor 2016	409-1 Operations and suppliers at significant risk for incidents of forced or compulsory labor	p.35
GRI 416 Customer Health and Safety 2016	416-1 Assessment of the health and safety impacts of product and service categories	p. 46
	416-2 Incidents of non-compliance concerning the health and safety impacts of products and services	p.53

GRI Standard	Disclosure	Location
GRI 417 Marketing and Labeling 2016	417-1 Requirements for product and service information and labeling	p. 46
	417-2 Incidents of non-compliance concerning product and service information and labeling	p. 46
	417-3 Incidents of non-compliance concerning marketing communications	p. 46
GRI 418 Customer Privacy 2016	418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data	p. 53

Topics in the applicable GRI Sector Standards determined as not material

Topic	Explanation
GRI 301 Materials	The Company does not engage in material-intensive production as its core operations focus on software development, IT consulting, and cybersecurity services.
GRI 303 Water and Effluents	The Company operates in the digital and cybersecurity sector, with no water-intensive processes or industrial operations.
GRI 304 Biodiversity	The Company's operations are entirely digital and office-based, with no direct interaction with natural habitats or impact on biodiversity.
GRI 306 Waste	The Company's operations are primarily digital and office-based, generating minimal waste.
GRI 308 Supplier Environmental Assessment	The Company operates in the digital and cybersecurity sector, with limited environmental impact from its suppliers. Since the supply chain primarily consists of technology providers, software vendors, and professional service firms, there are no significant environmental risks requiring formal supplier environmental assessments.
GRI 411 Rights of Indigenous People	The Company operates in the digital and cybersecurity sector, with no activities affecting Indigenous communities.
GRI 413 Local Communities	The Company operates in the digital and cybersecurity sector, with no direct physical impact on local communities.
GRI 414 Supplier Social Assessment	The Company primarily engages with technology providers, software vendors, and professional service firms, which do not pose significant social risks.
GRI 415 Public Policy	The Company does not engage in political activities, lobbying, or policy advocacy. It remains neutral in political matters and does not provide financial contributions or support to political parties, policymakers, or related organizations.
GRI 203 Indirect Economic Impact	The Company operates in the digital and cybersecurity sector, where indirect economic impacts are not easily quantifiable in traditional terms.
GRI 410 Security Practices 2016	The company does not employ physical security personnel, and its operations are focused exclusively on digital environments with no significant human rights risk related to security practices.

GRI Statement of Use

At Group-IB, we are committed to transparently communicating our ESG performance to our stakeholders. This commitment aligns with our sustainability approach and reflects our role in addressing global challenges, including those outlined in the United Nations SDGs.

As a cybersecurity company, we recognize that sustainability extends beyond environmental stewardship, as it encompasses digital resilience, data privacy, ethical governance, and social responsibility. This document serves as our Statement of Use regarding the GRI Standards, the world's most widely recognized framework for sustainability reporting. The GRI Standards enable us to report non-financial performance with rigor and accountability, ensuring we uphold the same standards of integrity that define our cybersecurity solutions.

GRI Standards Used

We have used the GRI Standards in our reporting process, focusing on disclosures that are material to our business operations and stakeholders. Such an approach ensures that we address the areas where our impact is most significant, including data security, privacy protection, ethical governance, and workforce well-being. Our reporting aligns with our broader business strategy and sustainability commitments, reinforcing the trust that underpins our relationships with clients, partners, and communities.

Material Topics

The Material Topics identified in our Sustainability Report have been determined through a comprehensive materiality assessment involving engagement with both internal and external stakeholders. For cybersecurity companies, material topics often include cybersecurity risk management, data protection, regulatory compliance, employee development, and environmental impact related to IT infrastructure, all of which applies to us. The materiality assessment process helps us prioritize issues that have significant economic, environmental, and social impacts and that influence stakeholders' decisions.

Stakeholder Engagement

Stakeholder engagement is integral to our sustainability strategy and reporting process. We engage with a wide range of stakeholders (including clients, employees, regulators, investors, and industry partners) through various channels in an effort to understand their expectations and concerns regarding our ESG performance. Such feedback informs our materiality assessment, strategic decisions, and reporting priorities, ensuring that we remain responsive to evolving cybersecurity and sustainability challenges.

Commitment to Continuous Improvement

We are committed to continuously improving our cybersecurity practices and sustainability performance. Feedback from stakeholders is invaluable to this process and helps us refine our ESG performance and reporting practices. We welcome comments and suggestions regarding our sustainability efforts as we strive to help create a secure, ethical, and resilient digital future.

Fight Against Cybercrime

GROUP-IB