CYBERARK®
The Identity Security Company

Environmental, Social & Governance (ESG) Report

Fiscal Year 2023

Table of Contents

Letter from our CEO

2023 was a momentous year for CyberArk. With our excellence in execution and the strength of our identity security platform, we solidified our position as the leader in identity security and posted record results. We continue to deliver against our mission to secure the world against cyber threats so together we can move fearlessly forward. Every word in that mission statement is carefully curated, and "Together" was chosen specifically because we cannot do this alone. From our customers to our partners to our employees, cybersecurity is a team effort. Across our employee base, 2023 was a year in particular where those core values were on prominent display. The war in Israel, following the attacks on October 7th, has affected our employees, their families, friends, colleagues and entire communities. Within CyberArk, we are in this together, and every CyberArker exemplified our core value "We" this year. The core values of our organization were at the forefront of our collective mind as our team navigated adversity, and I am immensely proud of how our team globally, and in Israel in particular, has come together to support each other. As I think about the year, it was one of great accomplishment juxtaposed against great tragedy and loss. For CyberArk, "Together" took on even more meaning in 2023.

Organizations globally are facing an unprecedented increase in new human and non-human identities, across hybrid and multi-cloud environments, and seeing attacker innovation driven by emerging technologies like artificial intelligence (AI). While each breach is unique, we continue to see evidence that there is one constant in cyberattacks: all roads lead to identity. In that context, it is no surprise customers gravitate towards a company like CyberArk, with security at the heart of its DNA, and a long track record of defense-in-depth innovation. The mission-critical nature of our platform helps us achieve our vision of securing every identity with the right level of privilege controls.

We were also proud of the steps we have continued to take in advancing our Environmental, Social and Governance (ESG) priorities as we move forward in addressing the needs of and creating long-term value for our stakeholders. In 2023, we conducted an ESG impact analysis for the second time, incorporating perspectives from various stakeholders, including employees, customers, and investors, to better understand how ESG-related risks and opportunities can impact our business and align our efforts with our broader company strategy.

Recognizing every organization's responsibility towards the environment, we continue to make progress in evaluating our carbon footprint. In 2023, we obtained third-party verification of our Scope 1 and Scope 2 greenhouse gas (GHG) emissions to a limited level of assurance and started measuring our Scope 3 emissions for the first time. We plan to use this evaluation as a starting point to explore ways to further reduce our environmental impact.

As a global technology company, our people are the cornerstone of our success. It is our firm belief that a diverse and inclusive workforce that is empowered to be the best and most authentic version of themselves is central to achieving our business outcomes. In 2023, we increased our focus on providing role-specific training on various topics to upskill our colleagues, enabling them to excel in both current and future roles. In our commitment to fostering a culture of belonging, we are excited to see a significant increase in engagement across our three Employee Resource Groups (ERGs), which are focused on empowering our people across various aspects of identity.

As a cybersecurity company, our customers rely on CyberArk as a trusted partner, and it is our duty to lead the way on governance to ensure CyberArk is built to last. Both our management team and the Board of Directors (Board) remain committed to driving progress in areas like board diversity, as well as our ongoing efforts on Ethics and Compliance, to uphold the highest standards of integrity in our business. In November 2023, the Board announced the appointment of Mary Yang as a new director, bringing key expertise in areas such as competitive analysis, strategic execution and cybersecurity. The Board's goal is to introduce a new director at least once every five years to ensure strong independence and inclusion of diverse backgrounds, skills, experiences and perspectives that are essential for effective oversight.

CyberArk's commitment to advancing sustainable practices in our business is ongoing, and we will continue to take a Fearlessly Forward approach to ensure that we are always improving and advancing.

I would like to express my gratitude to our employees, customers, partners and investors for their unwavering support towards our mission of building a safer and better world.

Respectfully,

Matt Cohen, Chief Executive Officer

"

In 2023, we continued to deliver on our mission of making the world more sustainable, by keeping our customers secure. In a year marked by both triumph and tragedy, our core value of 'We' was top of mind, exemplifying our amazing culture that prioritizes our employees' health, safety and well-being. Amidst these challenges, our dedication to advancing our ESG priorities was unwavering, reflecting our commitment to creating sustainable, long-term value for our stakeholders."

Udi Mokady
Founder and Executive Chair

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Business Overview

Securing every identity matters.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Mission
Secure the world against cyber threats so together we can move *Fearlessly Forward*.

Vision
Every identity secured with the right level of privilege controls.

CyberArk is a global leader in identity security, centered on intelligent privilege controls, with a focus on protecting organizations against identity–based cyberattacks. We apply intelligent privilege controls to all identities — human and machine — with continuous threat detection and prevention across the entire identity lifecycle. With CyberArk, organizations can enable Zero Trust and least privilege with complete visibility, so that every identity can securely access any approved resource, located anywhere, from everywhere – all on our CyberArk Identity Security Platform.

Our mission remains our North Star and highlights the key elements of our strategy. First, in order for us to be ready for the current and future threats that the world faces, we must have a relentless focus on security. Second, we are all in it together. All of us here at CyberArk, as well as our partners, and customers, must come together to achieve this mission. Our mission conveys why our work matters, and it is an important element of why we work at CyberArk.

Industry statistics

89%
of CIOs expect security spending to increase in 2024

73%
plan to implement or are testing generative AI

2.4x
annual growth in human and machine identities

No. 1
Credential theft remains the number one concern for cybersecurity professionals

99%
of security professionals agree they will face an identity-related compromise in the year ahead

Source: CyberArk 2023 Identity Security Threat Landscape Report

6

CyberArk at a Glance

>8.8K
global customers

>3K
employees across
>15
global offices

$774M
Annual Recurring Revenue (ARR)
Growth of 36% year-over-year

1999 founded

CYBR Nasdaq

Office locations

★ Israel | Germany | Australia
★ Americas | Spain | Singapore
UK | Netherlands | Japan
Canada | Italy | India
France | Turkey | Denmark

$752M
Revenue in 2023:
60% Americas
30% EMEA
10% APJ

Highly predictable model, with
>90%
of Revenue was Recurring in 2023

Only company with an end-to-end identity security platform

>$50 Billion
Total Addressable Market

Best Places to Work

BDi CODE

Great Place To Work Certified

BOSTON BUSINESS JOURNAL
BPtW
2023 BEST PLACES TO WORK

UK and Singapore locations

ESG Scores

MSCI ESG RATINGS AA
CCC B BB BBB A AA AAA

Corporate ESG Performance Prime
RATED BY ISS ESG▷

17.4
Low risk Sustainalytics score

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Our Core Values serve as the basis for our culture and choices that we make.

Trusted Experts

Demonstrate thorough expertise and knowledge within your specific field. Make proactive and continuous efforts to remain current in the latest product, industry or professional trends. Take action needed to win and sustain the customer's confidence.

Continuous Improvement

Demonstrate openness to constructive criticism and strive for continuous personal improvement. Perceive change as an opportunity and translate that approach into actions. Constantly seek ways to improve work processes.

Innovators

Re-imagine and accelerate new ideas, transforming concepts into market-leading solutions. Seek diverse perspectives and think differently to solve complex challenges, while maintaining a security-first mindset.

Smart, Bold but Humble

Strive to provide the best solutions for solving problems, based on deep knowledge, experience, logic, intuition and good intentions. Always maintain a modest and respectful approach.

We

Engage respectfully with others, maintaining good working relationships. Act as a team player and show willingness to assist colleagues, thereby contributing to achievement of team goals.

Customer First

Understand, anticipate and respond to the needs of customers. Provide high quality outputs focused on the customer's desired results. Exhibit strategic thinking for leveraging customer potential and customer success.

What's Best for CyberArk

Display open-mindedness and tolerance for others and others' opinions. Conduct yourself according to the company's best interests with appreciation for the broader picture.

Driven to Win

Apply determination and energy, going above and beyond, to achieve the desired result. Demonstrate full accountability to complete day-to-day tasks, as well as to solve complex challenges that power the company's success.

CEO Letter | Business Overview | Governance | Cybersecurity and Data Privacy | Our Culture and Talent | Communities | Environment | Appendix

CYBER**ARK**®

ESG at CyberArk

Security matters to strengthen sustainability. We are a leader in identity security, and our work has a clear purpose: to create a more secure world that helps protect our customers from the damage of cyberattacks. Identity is one of the most frequently exploited attack vectors, and the threat landscape is among the most severe in history. It is no surprise that credential theft remains the number one concern for cybersecurity professionals. Our solutions help our customers build more sustainable businesses by empowering them to securely execute their strategies. As a leader in our industry, we strive to extend our purpose beyond our own mission and the solutions we provide to customers. We are committed to making a positive impact with our employees, customers, partners and shareholders.

Being a leader means remaining steadfast in our values. Our values are the foundation of everything we do and are integrated into our operating rhythm. The principles of our ESG Program include:

Engagement: Communicating and seeking feedback from internal and external stakeholders

Transparency: Maintaining trust through disclosure and honest discussion about our progress

Progress: Making measurable and sustainable progress on focus areas that are most impactful to our business and stakeholders

ESG Highlights

33%
of Board members are women

92%
of employees completed cybersecurity and privacy training
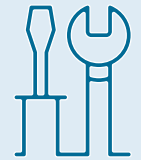
30,040
hours of learning & development across the company

Obtained **independent verification** of Scope 1 and Scope 2 GHG emissions (to limited level of assurance)

Since 2022, our employee survey response rate and engagement score have **increased**:

88%
employee survey response rate in 2023

81% in 2022

86%
engagement score in 2023

84% in 2022

9

🏠 CEO Letter **Business Overview** Governance Cybersecurity and Data Privacy Our Culture and Talent Communities Environment Appendix

CYBERARK®

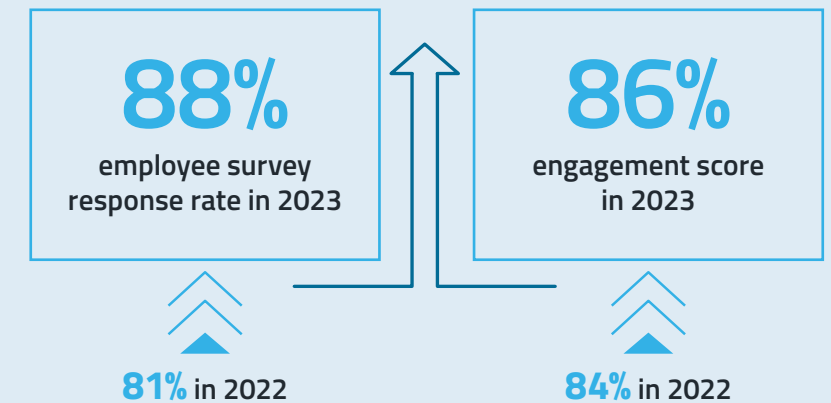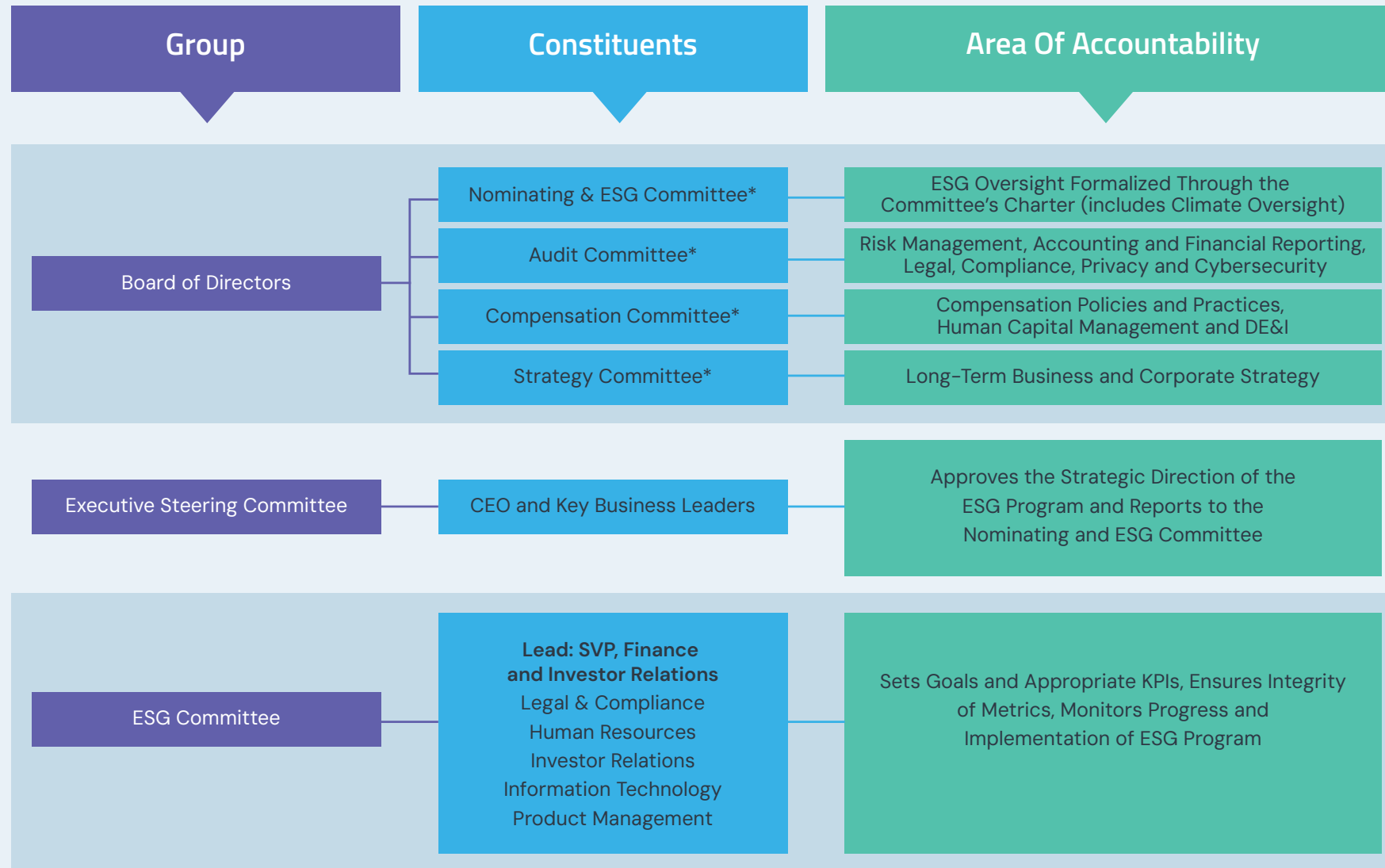| Group	Constituents	Area Of Accountability
Board of Directors	Nominating & ESG Committee*	ESG Oversight Formalized Through the Committee's Charter (includes Climate Oversight)
	Audit Committee*	Risk Management, Accounting and Financial Reporting, Legal, Compliance, Privacy and Cybersecurity
	Compensation Committee*	Compensation Policies and Practices, Human Capital Management and DE&I
	Strategy Committee*	Long-Term Business and Corporate Strategy
Executive Steering Committee	CEO and Key Business Leaders	Approves the Strategic Direction of the ESG Program and Reports to the Nominating and ESG Committee
ESG Committee	**Lead: SVP, Finance and Investor Relations** Legal & Compliance Human Resources Investor Relations Information Technology Product Management	Sets Goals and Appropriate KPIs, Ensures Integrity of Metrics, Monitors Progress and Implementation of ESG Program

*Board level committees share oversight of strategic initiatives

ESG Oversight

Effective oversight matters for accountability and transparency.

In 2021, we formally established an ESG Committee, which is led by the Senior Vice President, Finance and Investor Relations and comprises members of key business areas, including Legal and Compliance, Human Resources, Investor Relations, Information Technology, Product Management and Sales. The ESG Committee reports to an Executive Steering Committee that includes the Chief Executive Officer (CEO). The ESG Committee is overseen by the Board's Nominating, Environmental, Sustainability and Governance Committee (Nominating and ESG Committee) and the full Board. The Senior Vice President, Finance and Investor Relations has direct access to the Nominating and ESG Committee and reports on ESG matters and strategy on a semi-annual basis. We believe this structure increases the Board's effectiveness in overseeing the direction of the ESG strategy, as well as the establishment of KPIs and targets.

Focus Areas
Key ESG areas of Impact:

ENVIRONMENTAL

Energy and Emissions

Climate Change

SOCIAL

Health and Wellbeing

Retention, Engagement and Development

Diversity, Equity and Inclusion (DE&I)

GOVERNANCE

Data Protection and Privacy

Information Security and Oversight

Ethics and Compliance

Corporate Governance

Key ESG Topics

Insights matter to driving meaningful progress. In 2023, we conducted a second ESG impact analysis with direct input from key stakeholders, such as employees, shareholders and partners, in order to help us identify and prioritize key ESG focus areas. We also incorporated views from customers, the ESG rating agencies, and evaluated peers. Our ESG focus areas will support us in driving meaningful ESG business processes and progress, as well as ESG–related reporting. We understand that these ESG topics are dynamic and, therefore, will be evaluated periodically.

As the identity security leader, our work has a purpose: to create a more secure and sustainable world. Our ESG program supports our purpose by embedding the principles of sustainability into our business strategy, while providing transparency and establishing a dialogue with our customers, partners, suppliers and shareholders about the progress we are making in our ESG focus areas.

Governance, Ethics and Compliance

Good governance matters to business excellence.

Governance

As a leader in identity security, our customers see CyberArk as their trusted partner as they navigate a world with a heightened threat landscape. CyberArk is committed to effective corporate governance, with independent oversight by our Board. Our programs and policies are founded on the guiding principle that the Board is accountable for representing the best interests of our shareholders and also our other stakeholders, including employees, customers and partners. The Board also provides oversight of the sustainability and strategic initiatives that guide how we operate, protect and secure the company, preserve and enhance our culture, limit our impact on the environment and mitigate risk.

Board independence, diversity of experience and engagement with key stakeholders are essential to our success. From June 2016 until March 2023, the role of CEO and Chair of the Board was held by Mr. Udi Mokady, CyberArk's Founder. In April 2023, CyberArk separated the roles, with Mr. Mokady becoming Executive Chair and Matt Cohen, CyberArk's Chief Operating Officer, transitioning into the role of CEO.

We maintain a Lead Independent Director role with substantive duties and a direct line of communication to the executive team, senior leaders within the company and the Independent Auditor.

Our succession planning process includes ongoing Board-level training and rotation of senior leaders to various roles, and we are committed to maintaining a strong Board refreshment process. We implemented the goal to introduce a new Board member at least every five years to add new skills and promote a diversity of perspectives. When considering new Board members, we evaluate business expertise, industry experience, and diversity, among other considerations, and implement a robust selection process with the help of a third party to identify potential candidates.

In November 2023, Mary Yang joined our Board, while David Schaeffer's tenure on our Board concluded. Ms. Yang brings deep knowledge of cybersecurity, executive leadership, strategy execution, corporate development, and global M&A.

Board Composition*
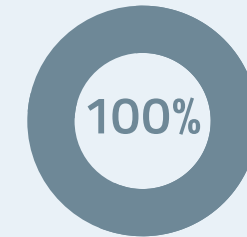
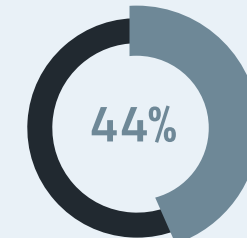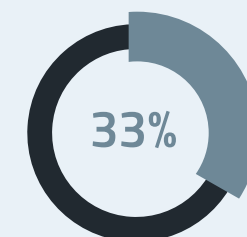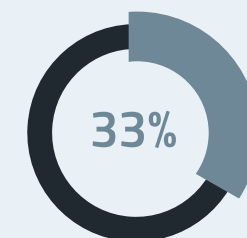**100%** Committee independence
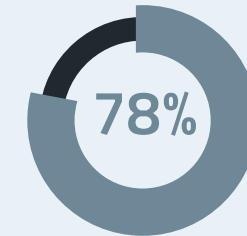
78% Board independence

44% of Board members are technology experts

33% of Board members are women

33% of Board members have a tenure of <5 years

*Percentages are approximate. As of December 31, 2023.

13

The director onboarding process includes a comprehensive and tailored set of sessions on our mission, values, and strategic goals, including ESG focus areas, as well as an in-depth understanding of the industry and competitive landscape. We also provide ongoing director education, including internally developed materials, presentations, and training as well as programs presented by third parties, to all our directors. In addition, we encourage our directors to attend CyberArk events, such as our annual IMPACT customer conference and our Global Kickoff employee event.

Risk Oversight

Our Board committees play a vital role in supporting the Board's risk oversight responsibilities. In order to facilitate new idea generation from rotated committee members, in 2022, appointed Mr. Auque and Ms. England to the Audit and Strategy Committees, respectively, and in 2024 appointed Ms. England to the Nominating and ESG Committee. The responsibilities of the committees are as follows:

Audit Committee
- Our overall risk assessment and strategy for managing enterprise risk
- Accounting and financial reporting, legal, compliance and privacy
- Cybersecurity, including product and information security
- Our Internal Audit team, led by our Head of Internal Audit, reports to the Audit Committee. The team provides an important oversight role and conducts periodic audits of major business processes, including appropriate legal and compliance processes.

Compensation Committee
- Compensation policies and practices related to our directors, executives and employees
- Our human capital management and diversity, equity and inclusion strategy

Nominating, Environmental, Sustainability and Governance Committee
- ESG program, including corporate governance and environmental (including climate) stewardship
- Succession planning

Strategy Committee
- Our long-term business and corporate strategy, including organic and inorganic growth

Stakeholder Engagement

Engaging with shareholders and other stakeholders is a vital part of our overall governance process. In addition to ongoing calls and attending conferences where we engage with investors in one-on-one sessions, twice a year we conduct specific outreach to engage in dialogue on matters such as strategy, corporate governance, compensation and ESG with our shareholders. During our engagement in 2023, the CEO, Executive Chair, Lead Independent Director, Chief Legal Officer, Senior Vice President, Finance and Investor Relations and Corporate Secretary participated in such conversations. Relevant feedback is shared with senior management, and periodic summaries are provided to the Nominating and ESG Committee and the full Board Areas of discussion during 2023 included board succession planning and engagement, committee composition and independence, artificial intelligence and business continuity planning.

For more information on corporate governance, including our discussion of executive compensation, please reference our Proxy Statement and Annual Report on Form 20-F for the fiscal year ended December 31, 2023.

Ethics and Compliance

Ethics matter as the cornerstone of trust. To continue delivering on our mission, it is critical that we conduct our business with the highest level of integrity. Our Governance, Ethics and Compliance strategy is overseen by our Chief Legal Officer and supported by our VP of Compliance and Ethics. We regularly review our progress with our CEO, our executive leadership team and the Audit Committee, which provides primary oversight of our Ethics and Compliance program.

Following the roll out of our new Code of Conduct in 2022, we continued enhancing our compliance and ethics program, which included updating policies and making them more user-friendly, targeted awareness raising for our employees, and active engagement on areas such as our open-door policy and the Speak Up Hotline.

Goals

Ongoing: All calls received through our Speak Up Hotline will receive an initial response within 72 hours.

While resolution time varies depending on the issue, unless a more complex investigation is required, we aim to resolve cases within one month of receipt.

2023 Goal progress:

1. We launched our new Code of Conduct e-Learning course to all existing employees as refresher training, and exceeded our goal of at least 90% completion rate within three months.

2. We conducted a training needs assessment to define a more targeted approach of how and to whom we deliver compliance and ethics training.

2024:

1. Continue raising employee awareness of CyberArk's Speak Up processes (including our confidential Hotline).

2. Conduct an ethics survey to obtain a deeper understanding of the ethics climate and relevant support needs in our business.

Our goal is for all calls received through our Speak Up Hotline to receive an initial response within 72 hours.

15

🏠 CEO Letter   Business Overview   **Governance**   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Code of Conduct

Our Code of Conduct (Code) applies to all executive officers, directors, and all other employees. We believe the Code aligns with our values and culture and practically addresses the compliance risks most relevant to our business and people. All CyberArk employees and executive officers were required to certify their compliance with the new Code when we launched it, during dedicated refresher training in 2023 and will continue to certify compliance with the Code and other compliance policies on an annual basis.

In parallel, our Vendor and Business Partner Code of Conduct outlines our expectations for upholding our high ethical standards, including complying with all applicable laws and regulations.

We encourage our employees to raise potential ethics concerns or Code violations to their manager or an internal specialist, such as Compliance or Human Resources, and have clearly communicated our zero-tolerance policy towards any type of retaliation against reporting employees and those who support an investigation. In addition, any person can report concerns and violations through an independent, confidential Speak Up Hotline, which is available 24/7 across all regions.

In addition to the Code, all employees and executive officers must comply with our compliance policies, including: Anti-Harassment & Anti-Discrimination Policy, Fair Disclosure Policy, Insider Trading Prevention Policy, Anti-Corruption Policy, Trade Controls Policy and Speak Up Policy. An overview of our key policies can be found here.

Training

We have an extensive training program to help guide and engage our employees in identifying and managing compliance and ethics risks. All new CyberArk employees are required to complete compliance training within 30 days of joining CyberArk, which includes a course on our Code as well as data security/privacy training. Ongoing, specific training is conducted on a variety of topics, including the Code, anti-corruption and bribery, insider trading, data privacy and cybersecurity.

We believe that targeted training, on top of baseline training, is imperative to conducting business in line with our legal obligations and upholding ethical, safe and secure workplace standards. In 2023, we conducted a training needs assessment to improve our approach to delivering compliance and ethics training. The results will inform our training strategy. Our aim is to make the training engaging, targeted and relevant based on an individual's role and geographic location.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Human Rights

CyberArk recognizes its important role in respecting human rights across the actions of its employees, vendors, suppliers, distributors, partners, business associates and third-party representatives. Our Human Rights Statement, the Code, UK Modern Slavery Statement and Vendor and Business Partner Code of Conduct clearly articulate our expectations regarding respecting the fundamental human rights of others.

Vendors and Business Partners

Our Vendor and Business Partner Code of Conduct states our expectations for vendors and business partners to comply with both the letter and the spirit of all laws, rules and regulations that apply to their businesses. We continue to enhance the way we onboard and manage our third parties to increase the efficiency and accuracy of our due diligence and to enhance compliance oversight, including anti-corruption and bribery and matters related to ESG.

Compliance with, and training on, our key governance policies is integral to our approach to conducting business with the highest level of integrity. An overview of our Policies can be found here.

CEO Letter   Business Overview   Governance   **Cybersecurity and Data Privacy**   Our Culture and Talent   Communities   Environment   Appendix

CYBER**ARK**®

Cybersecurity and Data Privacy

Securing the world against cyberthreats matters.

Approach

Data security matters to our people and customers. We believe security is a key pillar of an organization's value chain. As our customers' trusted security advisor, providing them with solutions to help protect every identity and stop cyberattacks, we are empowering them to move their businesses forward securely and sustainably. Therefore, we are committed to holding ourselves to strong security and privacy standards. Our Trust Center includes detailed information about our approach to cybersecurity and data privacy.

The Audit Committee of our Board of Directors has oversight of our cybersecurity risk management program, including product and information security. Our Audit Committee receives updates of our cybersecurity risks and controls from our management, at least on a quarterly basis.

In addition, our internal Information Security Steering Committee (ISSC) typically meets monthly to discuss key security matters, mitigation plans and progress. ISSC members include our CEO, Chief Information Officer (CIO), Chief Product Officer (CPO), Chief Legal Officer (CLO), and Chief Information Security Officer (CISO), as well as leaders from our Information Security, R&D and Security Services teams (including Red Team and cyber-attack experts), as needed. We also have a Service and Product Security Steering Committee (SPSSC) comprised of our CPO, Global Vice President (GVP) of R&D, Senior Vice President (SVP) of Product Management, CISO, Senior Legal Counsel and other security leaders from our Product Management, R&D and Information Security organizations.

Training

Internal training and awareness are a critical focus area of our cybersecurity risk management program. All employees and relevant contractors are required by policy to complete cybersecurity and data privacy training on an annual basis to build and maintain their knowledge and understanding on these topics. To augment and test our program's resiliency and support our employees in remaining vigilant, we conduct multiple educational campaigns, trainings and exercises throughout the year covering key aspects of security and data privacy, including role-specific training for relevant personnel and senior management. We update and align our training with ongoing security and legal developments.

Our internal Information Security Steering Committee (ISSC) oversees our network security, including new key security matters, mitigation plans and progress.

🏠 CEO Letter   Business Overview   Governance   **Cybersecurity and Data Privacy**   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Corporate and Product Security

Corporate Security

Holding ourselves to high standards matters to our success. CyberArk recognizes the importance of maintaining robust cybersecurity measures, and therefore, we have developed and implemented a cybersecurity risk management program intended to protect the confidentiality, integrity, and availability of our critical systems and information.

Our cybersecurity risk management program is centered on management of risks related to our network, product and cloud security, including security measures and controls to identify, protect, detect, respond to, and recover from cybersecurity risks. We use the National Institute of Standards and Technology (NIST) cybersecurity framework as a guide to help assess and improve our program. Our cybersecurity risk management program is integrated into our overall risk management process and shares common methodologies, reporting

channels and governance processes that apply across the risk management process to other legal, compliance, strategic, operational, and financial risk areas.

We conduct risk assessments and external audits on our corporate network at least annually, as well as security assessments by qualified third parties. CyberArk is ISO/IEC 27001:2022, ISO/IEC 27017:2015 and ISO/IEC 27018:2019 certified for Information Security Management Systems (ISMS). In addition, multiple of our software-as-a-service (SaaS) solutions received SOC 2 Type 2 and SOC 3 accreditation.

We also maintain an incident response plan and policy that includes procedures for responding to cybersecurity incidents and defines how security incidents are identified, classified, reported, remediated and mitigated.

We continuously work to enhance our cybersecurity posture through ongoing investments in technology, personnel training, and process improvement initiatives. We evaluate emerging threats, industry best practices, and regulatory requirements to adapt and strengthen our cybersecurity defenses. Our dedicated security teams work to improve our secure development, security operations and threat–mitigation practices.

Product Security

Product security matters to our customers' business resilience. With attackers continuously innovating, having an attacker mindset becomes increasingly critical in the development of our solutions. Our solutions support our more than 8,800 customers as they navigate the ever-expanding threat landscape to help them operate their businesses securely, safely, and sustainably.

Security and performance are built into our solutions and our practices, including:

- Developing and testing our solutions based on a Secure Software Development Lifecycle (SSDLC) process, while taking into consideration leading industry standards and guidelines including those published by NIST, Open Web Application Security Project (OWASP) and Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) framework;

- Embedding security experts and champions into our product development teams;

- Fostering a culture of security within the research and development teams through training programs;

- Using automated tools for Static Analysis Security Testing (SAST), Dynamic Application Security Testing (DAST) and Software Composition Analysis (SCA) for third–party dependencies scanning;

- Conducting external third–party penetration testing of our SaaS solutions annually;

- Conducting advanced penetration testing by an internal team based on a white–box methodology; and

- Implementing a rigorous vulnerability management process, overseen by our Product Security Office, which reports to the SPSSC, to monitor and prioritize security vulnerabilities identified in our solutions.

Our innovative solutions support our more than 8,800 customers as they navigate the increasingly complicated threat landscape, which gives them comfort to continue operating their businesses securely, safely and sustainably.

Data Privacy

Data privacy matters to being a trusted partner. We are committed to respecting personal data, including that of our customers, through appropriate use and storage and in compliance with applicable data protection laws. We also are committed to being transparent with our policies and practices as this is part of our trusted relationship with our customers. We maintain a global data protection compliance program aligned with applicable data protection laws, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This is reflected in our onboarding and ongoing management of third-party affiliates and partners to align our data flows and contracts with applicable laws and regulations. We continue to conduct annual privacy risk assessments to analyze our privacy standards across regions where we operate against GDPR requirements, as well as local privacy regulations, with the goal of incorporating best practices.

Transparency with our customers, our prospects and the public is important to maintaining a robust data protection culture and compliance program. The Privacy section of our Trust Center provides a comprehensive resource for customers and the public to access relevant information about how we process their data. Our Privacy Notice applies to all relevant business lines where we act as a controller of the information we process and covers topics relating to what data we collect, how it may be used, how a complaint can be reported and how individuals may opt-out. In 2023, we updated our Privacy Notice and also consolidated our Data Protection Customer FAQs, which covers how we handle our customers' data and encompasses all aspects of our SaaS solutions.

Other key accomplishments in 2023 include:

- Rolling out features for compliance with the Health Insurance Portability and Accountability Act (HIPAA) for new products and services falling within its scope.
- Achieving ISO 27018 certification.
- Enhancing our Privacy by Design and data-conscious culture through the development of an internal Privacy Ambassador program. The program designates people within key business units to receive enhanced training to become a subject matter expert.

Responsibilities include:

- Helping create data inventory for their respective business unit.
- Assisting with Privacy Impact Assessments for existing and new projects.
- Liaising with the Global Privacy team should business changes occur that impact policies or procedures.
- Informing and cultivating a deeper awareness on privacy within their business unit.

As we continuously drive progress and improvement, data privacy is a core initiative in our corporate strategy for the upcoming year.

Privacy Policies and Documents

Corporate Security Whitepaper →   Data Processing Addendum →

List of Sub-processors and Affiliated Entities →

Privacy and Data Protection Customer FAQs →

Privacy Center →   Privacy Notice →   Trust Center →

CYBER**ARK**®

Our Culture and Talent

People matter as the cornerstone of our business.

CEO Letter | Business Overview | Governance | Cybersecurity and Data Privacy | Our Culture and Talent | Communities | Environment | Appendix

CYBERARK®

Approach

Culture and talent matter to driving our long-term success. Our culture is an important contributing factor to our success and a key differentiator for CyberArk. We are committed to cultivating an environment where people feel valued and can build strong relationships that form the heart of the CyberArk community. We believe that by equipping and encouraging our people to achieve their full potential, we can successfully contribute to creating a safer, more secure world.

2023 was a year of contrasts. We had a momentous year from a business perspective, and we solidified our position as the leader in identity security. At the same time, the war in Israel affected our employees and their families, friends, colleagues and entire communities. The core values of our organization were top of mind as we came together to support each other as we navigated a time of tragedy and loss. Our employees' health, safety, and wellbeing were our top priority, and we came together to support them in numerous ways, including by continuing to provide meals and flexible work accommodations. This year, we also expanded access to mental health resources, in particular counseling, to help with stress and traumatic events.

Our People strategy is built on our four pillars: Attract, Belong, Communicate and Develop (ABCD). The ABCD strategy supports the wellbeing, retention, and career development of our people, since our culture continues to be a key ingredient in our success. We believe that the combined experience across the ABCD pillars, combined with the right tone at the top, enables our employees and our culture to thrive. Given its importance to our overall strategic execution, our human capital management and DE&I program is overseen by the Compensation Committee of the Board. Our CEO and our Chief Human Resource Officer regularly report to the Board and the Compensation Committee on human capital and DE&I matters.

We are proud that our comprehensive approach to our culture and employees has resulted in consistent recognition across several regions as a **"Great Place to Work"** by independent third-parties.

3.9%
voluntary turnover in 2023

7.9% in 2022

8.5%
overall turnover in 2023

11.7% in 2022

BDi CODE

Great Place To Work® Certified

UK and Singapore locations

BOSTON BUSINESS JOURNAL
BPtW
2023 BEST PLACES TO WORK

CEO Letter Business Overview Governance Cybersecurity and Data Privacy **Our Culture and Talent** Communities Environment Appendix

CYBERARK®

Wellbeing*

Wellbeing matters for every employee. We provide our employees and their families with robust healthcare benefits and a variety of health and wellness programs.

Our ongoing initiatives reflect a holistic approach that includes a variety of resources for employees, such as Employee Assistance Program (EAP) services in each region, meditation sessions, mental and physical wellbeing opportunities, corporate and regional employee newsletters and generous paid time off. In addition, ongoing training and wellness programs, including lectures, teambuilding opportunities, physical fitness classes provide support for physical, social, emotional and financial wellbeing.

We recognize that employees have varied needs and preferences for working; therefore, we offer hybrid working models, allowing employees and managers to determine the most suitable work arrangements for their teams. We offer in–person lunches and other programs that encourage connection and engagement as part of our flexible working arrangements.

We introduced new initiatives to help support our employees' mental health and wellbeing as part of our ongoing commitment to our employee base. This included a wellbeing platform that gives employees access to mental health resources on a confidential basis. We offered tailored webinars for employees in Israel, as well as for programs to provide support and guidance for managers with teams in Israel. Additionally, in the U.S., we hosted a webinar on wellbeing, which was closely aligned with our wellness program.

Our Core Values guide our actions as we set a strong tone of inclusivity, empowerment, and authenticity throughout our global teams.

*Benefits vary by region.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   **Our Culture and Talent**   Communities   Environment   Appendix

CYBERARK®

Attract: Recruitment

Attracting the right people matters for our culture.
In order to best serve our customers and to grow in the fast-moving cybersecurity industry, we require a diverse range of qualified people to continue our innovation in product development. Our recruitment strategy includes a variety of methods to attract a qualified and diverse range of candidates. Once hired, our structured onboarding and training process sets a positive direction for our new employees as they begin their CyberArk journey.

Hiring and training early-career talent / recent college graduates helps us diversify our employee base and is a key component of our recruitment program. Our U-Code program in Israel was created to focus on recent graduate hires into our 14-week training program before they transition to full-time roles within our team. U-Code program members have formed a close, collaborative network that continues after completion of the program. In our Newton, MA office, we have an ongoing college internship program, which includes students from Edinburgh through the Saltire Scholar

Program. In early 2023, we partnered with an external provider in Singapore to offer internship roles to university students nearing graduation, and we have a college graduate recruitment program in our Hyderabad, India office. Across all these programs, students gained invaluable first-hand work experience while contributing to a variety of teams, including R&D, Customer Support, Marketing, Sales, Information Technology, Human Resources and Finance.

Our commitment to recruitment also includes our approach to compensation. We conduct periodic gender pay equity analyses, offer stock-based compensation and the opportunity for all eligible employees to enroll in an Employee Share Purchase Plan (ESPP). Other benefits include competitive base salaries, variable pay programs to drive target achievements, paid time off, and generous leave for new parents regardless of gender. We regularly review our total compensation offerings to address evolving trends and developments in the complex global and local markets in which we operate.

Belong: Diversity, Equity and Inclusion

A diverse CyberArk matters to drive innovation. DE&I is critical to the successful execution of our strategy. An important focus for CyberArk is nurturing a culture of belonging where every voice is heard and appreciated. We believe this enhances decision-making, allowing for a forward-looking approach to creating solutions for our customers, thereby building a strong CyberArk.

The Compensation Committee of the Board, and ultimately the full Board, has oversight of our DE&I approach. Globally, our diversity initiatives are focused on gender representation; on a regional level, particularly in the U.S., we are focused on programs that support underrepresented racial and ethnic groups. Throughout 2022, we developed a new interview course for managers to raise awareness and advance inclusive hiring practices. We are pleased that more than 200 managers completed these training sessions in 2023.

Our ERGs are grassroots initiatives, empowering our employees to engage and support each other while helping advance our inclusive working environment. We currently have three ERGs: CYBR Women, a community connecting the incredible women at CyberArk, CYBR Pride, an LGBTQIA2S+ and ally community and CYBR Embrace, focusing on empowering employees across different elements of diversity, race, and abilities. Our ERGs saw a 50% increase in participation in 2023 compared to 2022, helping demonstrate the significance of their contributions to our employee experience.

CYBR WOMEN

CYBR PRIDE

CYBR EMBRACE

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBER**ARK**®

As part of our efforts to maintain inclusivity of hiring pools, in 2023, we continued to build out the Returnship program in the U.S. that we began in 2022, which is focused on helping potential job candidates (most of which are women) re-enter the workforce following a career break and includes specialized training for workforce returnees. For current employees, we offer a mentorship program for women, and a Boost Your Career program, which helps women build their personal brand, expand their network, establish career goals and balance work–life opportunities.

Other DE&I initiatives include:

- Working with an organization in Israel to recruit and support neurodiverse employees

- Conducting workshops for senior managers on inclusive behaviors and diversity as a business driver

- Offering training sessions on unconscious bias, allyship and inclusion

- Providing specialized training for our talent acquisition teams on inclusive hiring practices

---

In 2023, we published our second gender pay gap analysis for employees at our corporate headquarters in Israel. Overall, the findings of this analysis showed no meaningful differences in pay between male and female employees at various levels throughout the company.

CyberArk Today

27%
of employees are female
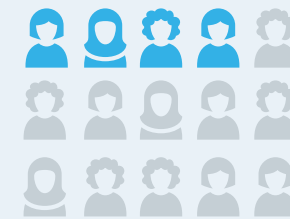
32%
of non-technical employees are female

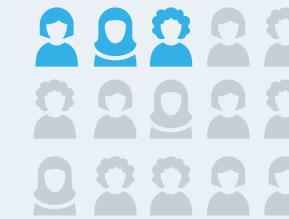**21%**
of technical employees are female

28%
of new hires are female

21%
of employees in the US are from traditionally underrepresented ethnic groups

211
managers completing inclusive hiring training

CEO Letter Business Overview Governance Cybersecurity and Data Privacy **Our Culture and Talent** Communities Environment Appendix

CYBER**ARK**®

Communicate: Engagement

Effective communication matters to foster engagement.
Two-way communication helps drive alignment and higher levels of employee engagement and satisfaction. Employees and leaders engage at our quarterly All-Hands meetings, a quarterly forum for leaders, and roundtable sessions that are aimed at increasing employees' business knowledge and transparency of strategy and progress. In addition, employees and their managers hold bi-annual feedback sessions to discuss achievements, challenges, and growth opportunities.

Employee feedback is an important consideration in shaping CyberArk's initiatives. Every year, we conduct an annual global employee survey using a third-party platform, which provides an avenue for honest and candid feedback that is received and analyzed by senior management. In our 2023 survey, our participation rate was 88%, an improvement compared to 81% in 2022's survey. The engagement score for our 2023 survey was 86%, an improvement from our 2022 score of 84% and well above the industry benchmark (76%).

This score highlights that the large majority of our employees were pleased with their overall experience and would recommend CyberArk to a peer. Based on the survey outcome, we identify opportunities, develop action items and hold employee roundtables to gather further feedback with the overall goal of improving employee experience, our culture, and our strategy. Areas of improvement that were identified in 2023 included increasing communication about CyberArk's business strategy, highlighting positive customer experiences across the organization and ensuring employees know about the programs offered to support career development and progression.

Employee engagement is also driven by regularly recognizing those who exemplify one or more of our Core Values. Our global recognition platform, introduced in 2021, provides opportunities for peer-to-peer rewards and also enables managers to provide real-time recognition to their team members.

Highlights from the 2023 Annual Global Employee Survey

86% Engagement Score (above industry benchmark of 76%)

88% Participation Rate (compared to 81% in 2022)

Develop: Learning and Development

Development matters to empowering growth.
CyberArk's people are intellectually curious, lifelong learners who often take part in programs outside of CyberArk, in addition to those offered by the company. We encourage all employees to shape their own learning journey and take advantage of the broad variety of self-paced, on-demand learning and development opportunities that we offer. We believe our focus on learning and development, opportunities for internal mobility, and career progression provides employees with opportunities to enhance their impact and contribute to their fullest potential in their current roles and in future roles. We deliver learning solutions using various platforms and methodologies, including classroom-based sessions, hackathons, virtual webinars, coaching, and experiential learning to meet the needs of our employees.

During 2023, we welcomed a new leader to our learning and development team in order to help enhance our program.

We aim to offer innovative approaches to employees that help them grow and develop in their careers. During 2023, we began to lay the groundwork for our new Career Lattice program. The program will provide tools to support employee career progression in a variety of ways — not only through promotions but also through expanding their current role. This includes equipping managers with tools to coach employees through the process.

Mid-career employees are offered training on enhancing verbal and written communication, cross-cultural collaboration, and time management skills. We also focus on developing and offering leadership programs for both junior and senior managers, on topics related to developing the business, in addition to helping our people develop.

100%
of employees received training

30

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   **Our Culture and Talent**   Communities   Environment   Appendix

CYBERARK®

Training

Instructor-led courses:

67 technical courses offered

841 participants in technical courses

Cloudguru:

2,133 hours watched

712 users using the platform

LinkedIn Learning:

2,597 courses completed

4,298 hours watched

We support employees in pursuing a variety of internal and external learning opportunities, including:

Offering an annual tuition reimbursement program for employees pursuing degree programs or certifications.

Providing every full-time employee with access to a set of technology, business and skill-building courses through our Learning Management System, as well as access to LinkedIn Learning, which offers thousands of self-paced and online learning opportunities.

Offering focused programs for our technical and non-technical team members, tailored to their job role and/or experience level.

We focus on building our talent pipeline and future leaders, offering a targeted curriculum that includes "Engage," "Elevate," and "Expand" programs for various levels of managers and emerging talent.

During 2023, we emphasized training on security and cloud-related topics.

Technical employees participated in security training tailored to their roles and departments. While all technical staff received fundamental security training, the extent of additional training varied based on specific job responsibilities. We also started a new program on service excellence for people working with customers, such as solutions engineers.

In 2023, we saw an increase in the number of employees participating in our learning and development offerings, as we added more courses and standardized various programs across the company. We will continue to enhance and advance our training programs to help our colleagues learn and fulfill their potential.

To enhance our internal offerings, CyberArk also partners with educational institutions to help deliver training sessions for our employees. In 2023, we partnered with Babson College, a school of business and entrepreneurship in Greater Boston and the Interdisciplinary Center Herzliya (IDC), also known as Reichman University, in Israel.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Communities

Supporting our communities matters to collective progress.

Approach

Participation matters to fostering connection with our communities. We believe that getting involved and giving back are vital aspects of being part of a community. CyberArk contributes time, expertise, and resources to global and local community initiatives. Our global efforts are primarily focused on environmental improvements within our communities, DE&I initiatives, improving community members' access to basic needs, such as food and clothing, and improving access to and helping advance careers in technology.

Our Chief Human Resources Officer oversees CyberArk's group-wide participation in community efforts.

Our global efforts are primarily focused on environmental improvement within our communities, DE&I initiatives and improving access to and the advancement of careers in technology.

Volunteering

Engagement matters to feel connected. Our teams prioritize making a positive impact by participating in hands-on initiatives. In 2023, globally, CyberArk employees volunteered at various events that support areas such as education, basic needs, support for those living with cancer and disaster relief.

In addition to helping build team unity and engagement, our volunteering programs provide support to benefit organizations in each of the locations in which we operate, such as Cradles to Crayons, Cyber Education Center, Eliya, Facing History & Ourselves and The Global Food Banking Network, among others.

In 2023, our employees continued their volunteering efforts across various initiatives, while we also expanded our support for new initiatives. In America, our team continued to sponsor a virtual 5k run for Catie's Closet, a non-profit providing free, in-school access to clothes and basic necessities for New England students in need.

Two new initiatives our employees volunteered for in 2023 were Girl Scouts of the USA and the Charles River Watershed Association Earth Day Clean Up event. Our CYBRWomen ERG launched a community education initiative developing materials and a program to teach Girl Scouts cyber safety basics so they are able to earn cybersecurity badges.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBER**ARK**®

Key volunteering initiatives

Charles River Watershed Association Earth Day Clean Up

45 volunteer hours

AMERICAS

Cyber Youth – Raising awareness on cyber–wellness in local schools

22 volunteer hours

APJ

Clearing of invasive species to encourage biodiversity and to build bug houses

30 employees

EMEA

Touch Home Care – Emergency Food Ration Packing

920 emergency ration packs packed

APJ

In commemoration of Rosh Hashanah, our Petach Tikva and Beer Sheva offices held a family community responsibility event collecting and donating groceries to families in need

126 volunteer hours

ISRAEL

Heritage site clean up

10 employees

ITALY

*Number of volunteer hours refers to the volunteering initiatives listed

Financial Support and Donations

Giving back matters to building trust.
We support many local and global organizations through corporate donations. This includes a key initiative where each employee has the option to donate to a charity of their choice following their one-year anniversary of employment. In addition, employees can donate to a variety of charitable causes, choosing to pay forward what they received as part of our broader employee recognition program. In 2023, both CyberArk and our employees continued to support a variety of charities located in the communities where we operate.

Some of the new initiatives we supported in 2023 include our employees and members of our executive team helping to raise funds for the Global FoodBanking Network. The funds raised by our employees provided 186,000 meals for those in need across the globe.

Team members also donated to support those in need after the devastating earthquake in Turkey.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBER**ARK**®

Environment

Managing our footprint matters to operating sustainably.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Approach

Our environmental impact matters to promote operational resilience/business longevity. Operating responsibly and strengthening our environmental program are the foundations of our sustainability program. In 2022, we conducted two climate-related strategy sessions with our Executive Leadership Team and business leaders from Investor Relations, Human Resources, Facilities, Legal, Compliance, and Operations, and we measured our Scope 1 and Scope 2 GHG Emissions. In 2023, we continued to build our understanding of our footprint to further inform how climate-related issues could impact our business. Engagement with customers has also been a key component of building our environmental strategy.

We continue to take steps in measuring and evaluating ways to reduce our impact on the environment and how climate change-related risks and opportunities can impact our business.

Climate Change

Measuring our climate impact matters to enhancing our environmental stewardship.

Governance, Strategy, Risk Management. Our climate strategy continues to evolve and is developed from the bottom up with the Nominating and ESG Committee having primary oversight over our environmental stewardship as part of the ESG program. Climate-related issues are a specific area for which the Committee reviews progress and approves future direction. During 2023, the Committee reviewed the measurement and data verification of our Scope 1 and Scope 2 GHG emissions, as well as our intent to develop a GHG emissions reduction strategy in the coming years. In addition, the Committee reviewed the level of engagement we are having with customers and partners regarding our environmental program.

In order to better understand and assess the climate-related risks and opportunities facing our business and establish a climate strategy, we conducted two corporate-level climate strategy sessions in 2022. The goal of the first session was to better understand the market drivers for climate-related impacts and the importance to CyberArk of understanding our climate impact to assess potential business risks and opportunities.

37

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBER**ARK**®

With this enhanced understanding, the group held a second session, facilitated by a third party, which focused on the specific transition and physical climate-related risks that have the greatest potential to impact CyberArk's business by 2025. Included was a climate scenario analysis that aligned with the Network for Greening the Financial System (NGFS) Climate Scenarios, which, while developed primarily for central banks, are also recognized as useful to the broader financial and corporate communities.

Overview of key risks assessed in our Climate Strategy Sessions:

- **Transition risks:** Policy and Legal, Technology & Market, and Reputation

- **Physical risks:** Acute and Chronic

Reference scenarios used:

No Mitigation: Global climate action stagnates, leading to unchecked emissions increases and limited action to avert physical risks.

Stated Policy (business as usual): Measured progress on climate action, resulting in some reductions and avoidance of worst effects of climate change.

Paris ambition 1.5C: Coordinated aggressive policies + action to address emissions and physical risks.

Boundary conditions:

- Forecast to 2025
- Operational boundary: Global Operations, Scopes 1–3

The analysis found that, overall, climate-related risks pose a low risk to CyberArk's business and operations in the near- to medium-term, affirming we are well-positioned to align and adapt to the transition to a low carbon economy. However, we continue to monitor these developments and integrate considerations into business planning where necessary. For example, when conducting data center planning, we consider the environmental footprint and our overall computing capacity, which includes having over 85% of our applications as SaaS. Most of our IT infrastructure runs in a public cloud environment operated by third parties, who are able to achieve greater efficiencies of scale, including in the use of clean energy sources, than we would be able to achieve operating such data centers on our own.
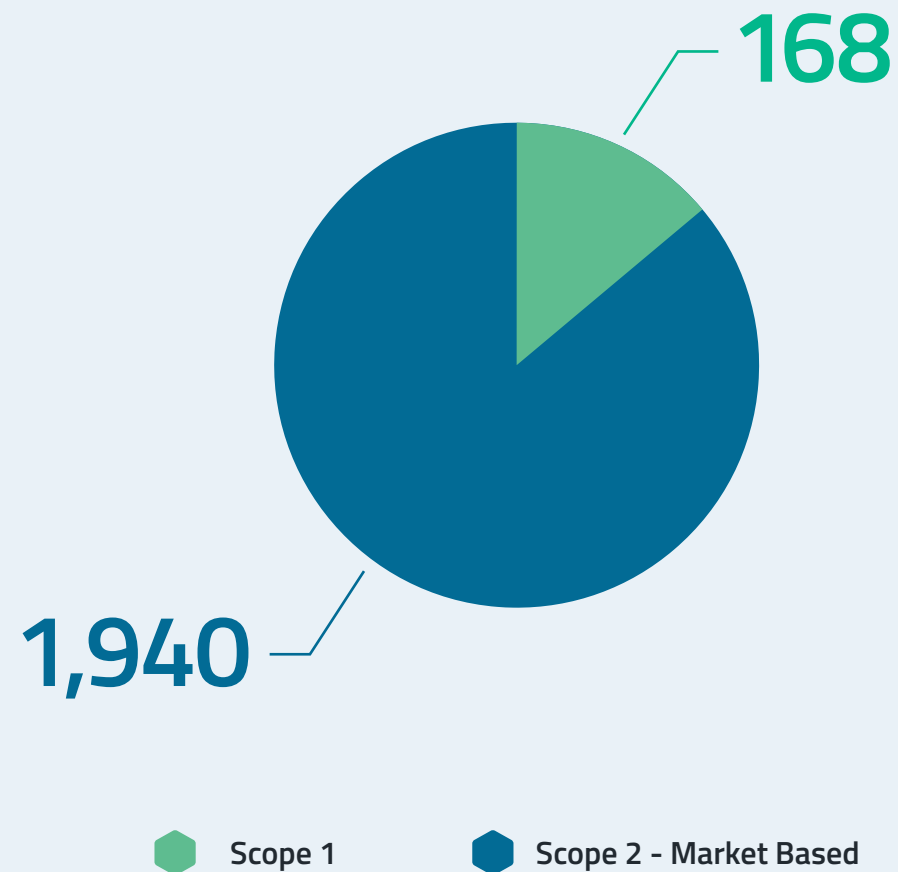
CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

Climate-Related Scenario Analysis: Risk Summary

Transition Risk Types

Policy & Legal

Technology & Market

Reputation

Physical Risk Types

Acute & Chronic

	No Mitigation	Stated Policy	Paris Ambition: 1.5C
Policy & Legal	Low Impact	Low/Moderate Impact	Moderate Impact
Technology & Market	Low Impact	Low Impact	Low Impact
Reputation	Low Impact	Low Impact	Moderate Impact
Acute & Chronic	Low Impact	Low Impact	Low Impact

The analysis helped us understand and more fully assess how climate-related risks should factor into our strategy planning. We believe that CyberArk's business and operations are well-positioned to align and adapt to the transition to a low carbon economy.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix

CYBERARK®

FY2023 Scope 1 & Scope 2 GHG Emissions (in mt CO_2e)

168

1,940

🟢 Scope 1   🔵 Scope 2 - Market Based

Metrics

Since 2021, we disclosed our Scope 1 and Scope 2 GHG emissions inventory annually. In 2023 we received independent, third-party verification of our FY 2022 Scope 1 and Scope 2 Location and Market-based emissions to a limited level of assurance.

Due to the importance of having a full scope of our footprint, during 2023, we completed a first quantification of 2022 Scope 3 emissions. Our quantification was expanded for FY 2023 to include additional, relevant categories. We received independent, third-party verification for FY 2023 Scope 1 and Scope 2 emissions.

Targets

CyberArk understands the value of setting climate targets as a tool to make meaningful progress in reducing our footprint. As such, we are continuing to work toward a strategy to reduce our emissions.

*During the process, for 2022, 2023 and going forward, we re-allocated emissions that are related to our shared (e.g., WeWork) offices to Scope 3. The majority of our Scopes 1–2 emissions is from purchased electricity within Scope 2.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   Appendix
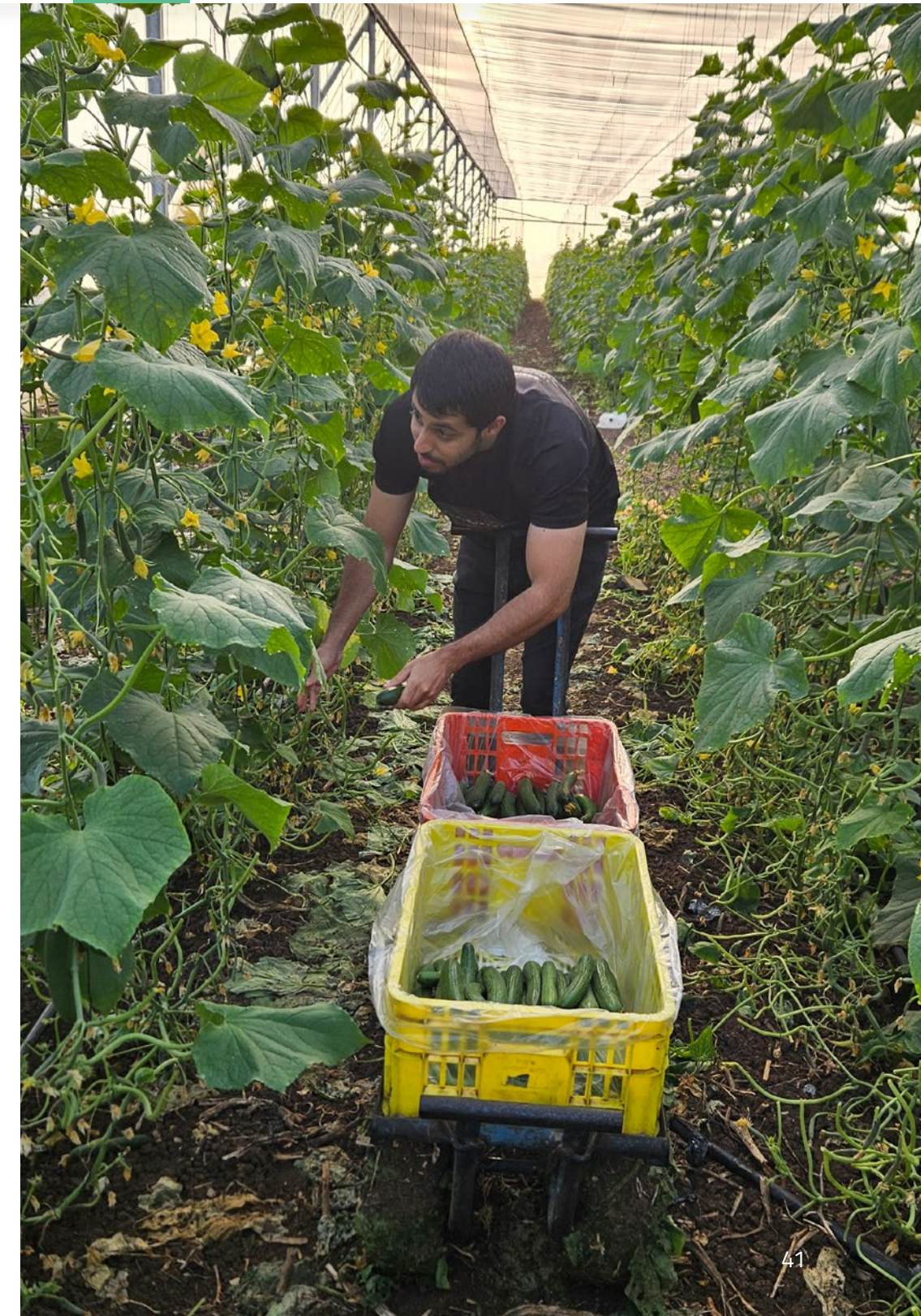
CYBERARK®

Engagement

Building awareness matters to expand our impact. Engaging employees on key initiatives is important to the long-term success of our environmental initiatives and can help employees think about their overall impact beyond their day-to-day work. 2023 was the third year in which we offered educational and interactive webinar sessions as part of our Green April initiative, aligning with Earth Day. Two webinars were hosted: one focused on food waste and one on climate change, CyberArk's footprint and steps the company is taking to reduce, and how employees can make a difference. The webinars had over 200 employee attendees. Sessions are led by a senior manager and include members of our ESG Committee and our Senior Vice President, Finance and Investor Relations. Additionally, we hosted our annual Green Challenge where employees compete to complete various environmental challenges.

CyberArk's two Green Teams, one in Massachusetts and one in Israel, are building a grassroots sustainability movement with the goals of inspiring and educating employees on sustainable habits, recognizing sustainability opportunities, setting personal examples of sustainability habits, and ultimately improving our corporate sustainability. Over the course of 2023, our Green Teams coordinated several activities, including cleaning Coogee beach in Australia, clearing brush in EMEA and collecting surplus produce for a foodbank in Israel. With a growing interest from colleagues, we will continue developing engaging activities tailored to each of our operating regions, which resonates with CyberArk's culture.

Another important employee engagement initiative is our planting of a tree for each new employee and offering employees the opportunity to plant trees as part of our employee recognition program. We are proud to have planted over 750 trees in 2023 alone.

CEO Letter   Business Overview   Governance   Cybersecurity and Data Privacy   Our Culture and Talent   Communities   Environment   **Appendix**

CYBER**ARK**®

Appendix

Corporate Policies, Documents and Other Information

Policies and Documents

Anti-Corruption Policy Summary →

Corporate Code of Ethics & Conduct →

Environmental Statement →

Fair Disclosure Policy →

Global Health, Safety & Wellbeing Statement →

Human Rights Statement →

Infection Control Guidelines →

Modern Slavery Statement →

Vendor and Business Partner Code of Conduct →

Whistleblower Policy →

Board of Directors Committee Charters

Audit Committee Charter →

Compensation Committee Charter →

Nominating and ESG Committee Charter →

Other Information

Articles of Association →

Trust Center →

The below information references the topics from Sustainability Accounting Standards Board's (SASB) Software and IT Services industry standard (now part of the IFRS Foundation).

Environmental Footprint of Hardware Infrastructure		
SASB Code	Accounting Metric	FY2023
TC-SI-130a.1	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	Data not available at this time.
TC-SI-130a.2	(1) Total water withdrawn, (2) total water consumed, percentage of each in regions with High or Extremely High Baseline Water Stress	Data not available at this time.
TC-SI-130a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	We leverage third-party public data centers to host the majority of our computing power. Hosting in third-party data centers lowers our overall impact on the environment, including our electricity usage and our HVAC systems. As we evaluate expanding our data center needs, we will primarily look to third-party public cloud computing. In addition, we have moved the majority of our applications to SaaS applications, which lowers our data center requirements and our impact on the environment. In total, approximately 87% of our applications are SaaS.

Data Privacy and Freedom of Expression		
SASB Code	Accounting Metric	FY2023
TC-SI-220a.1	Description of policies and practices relating to behavioral advertising and user privacy	We have general marketing policies regarding the processing of personal data. These do not relate specifically to behavioral advertising, as this is not relevant to our core business. However, our internal privacy policy requires the completion of data protection impact assessments in the event of significant future changes to our practices in this respect. For more information, please see the Privacy Policy and Trust Center.
TC-SI-220a.2	Number of users whose information is used for secondary purposes	Numeric response not applicable. Like many software companies, we gain insights into how our customers use our products by analyzing data generated through product use. This may be used for a variety of purposes, including to help the customer optimize their use of the service and to recommend additional services. We do not sell this data to third parties — for example, for marketing purposes.
TC-SI-220a.3	Total amount of monetary losses as a result of legal proceedings associated with anticompetitive behavior regulations	None
TC-SI-220a.4	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	None
TC-SI-220a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	Data not available. To our knowledge, there is no country, where our core products or services have been subjected to government, that requires monitoring, blocking, content filtering or censoring within same country. We are not able to provide an analysis of whether any laws exist in any given territory that might render such action possible. Separately, we are precluded from providing certain products and services pursuant to Israeli and U.S. laws and regulations in certain countries.

*All data as of December 31, 2023.

Data Security		
SASB Code	Accounting Metric	FY2023
TC-SI-230a.1	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected	We have not sustained a personal data breach triggering obligations to notify either the individuals concerned or any government authority. See also "Internal Cybersecurity" section on page 38 in our Annual Report on Form 20-F for the fiscal year ended December 31, 2023.
TC-SI-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	CyberArk's Risk Management Program is an ongoing process of identifying, assessing and responding to risk. To manage risk, we work to understand the likelihood that an event will occur, assess potential resulting impacts and respond to the risks by implementing security controls based on CyberArk's risk tolerance. CyberArk conducts formal risk assessments on its corporate network on an annual basis. CyberArk's Risk Management Program is based on ISO/IEC ISO 27001:2022 Information Security Management System Standard and follows the NIST cybersecurity framework. In addition, the results of our annual assessment are included in the annual mitigation plan, which is presented to and monitored by CyberArk's Audit Committee of the Board.

Recruiting & Managing a Global, Diverse & Skilled Workforce		
SASB Code	Accounting Metric	FY2023
TC-SI-330a.1	Percentage of employees that are (1) foreign nationals and (2) located offshore	(1) Approximately 1% (2) Approximately 31% of employees in Israel Approximately 35% in North America Approximately 15% in EMEA Approximately 17% percent in APJ Approximately 2% in LATAM
TC-SI-330a.2	Employee engagement as a percentage	88% of our employees participated in our 2023 employee engagement survey.
TC-SI-330a.3	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	Gender (1) 29% (2) 21% (3) 32% Ethnicity (1) 9% (2) 32% (US only) (3) 16% (US only)

*All data as of December 31, 2023.

CEO Letter | Business Overview | Governance | Cybersecurity and Data Privacy | Our Culture and Talent | Communities | Environment | **Appendix**

CYBER**ARK**®

Intellectual Property Protection & Competitive Behavior		
SASB Code	**Accounting Metric**	**FY2023**
TC-SI-520a.1	Total amount of monetary loss ($) as a result of legal proceedings associated with privacy	None

Managing Systemic Risks from Technology Disruptions		
SASB Code	**Accounting Metric**	**FY2023**
TC-SI-550a.1	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	Data not available at this time.
TC-SI-550a.2	Description of business continuity risks related to disruptions of operations	CyberArk has implemented a Business Continuity Management Program designed to reduce the effects of an interruption to its essential business activities and to recover from loss of Information Technology assets in the event of a natural, human or technological disruption caused by accidents, equipment failures, deliberate actions or other occurrences. The continuity program aligns to industry standards and contractual requirements. For more information, please see the risks outlined in our Annual Report on **Form 20-F** for the fiscal year ended December 31, 2023.

Activity Metrics		
SASB Code	**Accounting Metric**	**FY2023**
TC-SI-000.A	(1) Number of licenses or subscriptions, (2) percentage cloud based	(1) $493 million in software licenses or subscription revenue (2) 63% of software licenses and subscription revenue was cloud based
TC-SI-000.B	(1) Data processing capacity, (2) percentage outsourced	Data not available at this time.
TC-SI-000.C	(1) Amount of data storage, (2) percentage outsourced	(1) Data not available at this time (2) ~87% outsourced

*All data as of December 31, 2023.

Cybersecurity and Privacy

Metric	FY2023
# of hours in cybersecurity/data privacy training (average)	1–2 hours
# of SaaS solutions received SOC-2 Type II certification	8
% of outsourced data storage	~87%
% of employees trained on cybersecurity/data privacy	92%

Governance

Metric	FY2023
% of independent board members	78%
% of independent standing Board committees	100%
% of women on the Board	33%
# of women on the Board	3
Total amount of monetary losses as a result of legal proceedings associated with anticompetitive behavior regulations	None

People

Metric	FY2023
% of new hires that are women	28%
% of employees that are foreign nationals	1%
% of ethnically diverse employees in the US (under-represented ethnic groups)	21%
% of ethnically diverse employees in management	9%
% of ethnically diverse employees in technical roles (US only)	32%
% of ethnically diverse employees in non-technical roles (US only)	16%
% of women in management	29%
% of women in technical roles	21%
% of women in non-technical roles	32%
% of women across the company	27%
% of employees (in Israel)	31%
% of employees (in North America)	35%
% of employees (in EMEA)	15%
% of employees (in APJ)	17%
% of employees (in LATAM)	2%
Employee by age band/generation band	20–29.9 – 15% 30–39.9 – 39% 40–49.9 – 31% 50–59.9 – 13% 60–70 – 2%

Metric	FY2023
% retention of new hires	95%
% of employees who have an annual or bi-annual performance review	95%
# of Employee Resource Groups	3
# of managers completing inclusive hiring training	211
% of participants in pulse surveys	88%
% of employee satisfaction	86%
% turnover (voluntary)	3.9%
% turnover (overall)	8.5%
Total # of hours of learning and development across the company	30,040
# of training technical courses on offer to employees	67
# of participants taking technical courses	841
# of hours watched using Cloudguru	2,133
# of employees using the Cloudguru platform	712
# of LinkedIn learning courses completed	2,597
# of hours watched in LinkedIn learning	4,298
# of employees completing the OSWAP training program	558
# of employees completing the Secure Code and Severity Assessment training program	639

*All data as of December 31, 2022.

Environment

Metric	FY2023
Scope 1 absolute emissions (mt CO_2e)	167.77
Scope 2 absolute emissions – market based (mt CO_2e)	1,939.65
Scope 2 absolute emissions – location based (mt CO_2e)	1,954.25
Scope 1+2 market based (mt CO_2e)	2,107.42
Scope 1+2 location based (mt CO_2e)	2,122.02
Emissions intensity per $m revenue – market based	2.6
Emissions intensity per sq.ft – market based	0.01
Emissions intensity per $m revenue – location based	2.6
Emissions intensity per sq.ft – location based	0.01
Number of trees planted	774

*All data as of December 31, 2023.

This report contains forward-looking statements, which express the current beliefs and expectations of our management. In some cases, forward-looking statements may be identified by terminology such as "believe," "may," "estimate," "continue," "anticipate," "intend," "should," "plan," "expect," "predict," "potential" or the negative of these terms or other similar expressions. Such statements involve a number of known and unknown risks and uncertainties that could cause our future results, levels of activity, performance or achievements to differ materially from those expressed or implied by such forward-looking statements. Important factors that could cause or contribute to such differences include risks relating to: changes to the drivers of our growth and our ability to adapt our solutions to IT security market demands; our sales cycles and multiple pricing and delivery models; our ability to sell into existing and new customers and industry verticals; an increase in competition within the Privileged Access Management and Identity Security markets; unanticipated product vulnerabilities or cybersecurity breaches of our systems or our customers' or partners' systems; complications or related to our subscription model, including uncertainty regarding renewals from our existing customer base and retaining sufficient subscription or maintenance and support service renewal rates; risks related to compliance with privacy and data protection laws and regulations; risks regarding potential negative economic conditions in the global economy or certain regions, including conditions resulting from financial and credit market fluctuations, rising interest rates, bank failures, inflation and the potential for regional or global recessions; our ability to hire, train, retain and motivate qualified personnel; reliance on third-party cloud providers for our operations and SaaS solutions; our history of incurring net losses and our ability to achieve profitability in the future; risks related to our ongoing transition to a new Chief Executive Officer; our ability to find, complete, fully integrate or achieve the expected benefits of strategic acquisitions; the duration and scope of the COVID-19 pandemic and its resulting effect on the demand for our solutions and on our expected revenue growth rates and costs; our ability to expand our sales and marketing efforts and expand our channel partnerships across existing and new geographies; risks related to sales made to government entities; regulatory and geopolitical risks associated with global sales and operations (including the current conflict between Russia and Ukraine) and changes in regulatory requirements or fluctuations in currency exchange rates; the ability of our products to help customers achieve and maintain compliance with government regulations or industry standards; risks related to intellectual property claims or our ability to protect our proprietary technology and intellectual property rights; and other factors discussed under the heading "Risk Factors" in our most recent annual report on Form 20-F filed with the Securities and Exchange Commission. Forward-looking statements in this release are made pursuant to the safe harbor provisions contained in the U.S. Private Securities Litigation Reform Act of 1995. These forward-looking statements are made only as of the date hereof, and we undertake no obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise. Furthermore, while future events discussed in this report may be significant, any significance should not be read as necessarily rising to the level of materiality of certain disclosures included in our SEC filings. Even if we use the word "material" or "materiality" in this report in relation to those statements or in other materials that we may release from time to time in connection with the matters discussed herein. Moreover, given the uncertainties, estimates and assumptions required to make certain non-financial disclosures, and the timelines involved, materiality is inherently difficult to assess far in advance. In addition, given the inherent uncertainty of the estimates, assumptions and timelines contained in this report, we may not be able to anticipate in advance the degree to which we will or will not be able to meet our plans, targets or goals. In addition, non-financial information, such as that included in parts of this report, is subject to greater potential limitations than financial information, given the methods used for calculating or estimating such information. Additionally, historical, current, and forward-looking environmental and social-related statements are based on standards and metrics for measuring progress, as well as standards for the preparation of any underlying data for those metrics, that are still developing and internal controls and processes that continue to evolve. For example, we note that standards and expectations regarding greenhouse gas (GHG) accounting and the processes for measuring and counting GHG emissions and GHG emission reductions are evolving, and it is possible that our approaches both to measuring our emissions and to reducing emissions and measuring those reductions may be, either currently by some stakeholders or at some point future, considered inconsistent with common or best practices with respect to measuring and accounting for such matters, and reducing overall emissions. While these are based on expectations and assumptions believed to be reasonable at the time of preparation, they should not be considered guarantees. If our approaches to such matters are perceived fall out of step with common or best practice, we may be subject to additional scrutiny, criticism, regulatory and investor engagement or litigation, any of which may adversely impact our business, financial condition, or results of operations. Separately, the standards and performance metrics used, and the expectations and assumptions they are based on, have not, unless otherwise expressly specified, been verified by any third party. In addition, while we seek to align these disclosures with the recommendations of various third-party frameworks, such as the Sustainability Accounting Standards Board, we ultimately use such frameworks only as references for our disclosures and cannot guarantee strict adherence to these framework recommendations. Additionally, our disclosures based on these frameworks may change due to revisions in framework requirements, availability of information, changes in our business or applicable governmental policy, or other factors, some of which may be beyond our control.

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

CYBERARK®
The Identity Security Company