PUBLICATION
MAY 2025

ADDRESSING CYBERSECURITY CHALLENGES IN THE AFRICAN CLIMATE IMPACT SECTOR

PERSISTENT

Triple Jump

BY
MAGDALENA HERMAN &
VINCENT KIENZLER[1]

ABOUT THE AUTHORS

MAGDALENA HERMAN

Magdalena is a Data and Technology Specialist at Persistent. She has broad experience across a variety of applications and IT set-ups, including inventory management, call centre software, CRM and more. She has worked on IT systems implementation, mobile apps configuration as well as data related projects with a variety of organizations across 3 continents with the main focus on Africa.

VINCENT KIENZLER

Vincent is Persistent's Lead Tech Venture Builder, working closely with partner companies to solve technology challenges, define tech strategy, and build capacity in software development, IT and cybersecurity, and product hardware. He has over 12 years of experience living and working in Sub-Saharan Africa and has co-founded two companies in the tech and energy sectors.

Africa's digitalization landscape is rapidly evolving, driven by increasing internet penetration, a growing tech-savvy population, and significant investment in infrastructure. While uneven connectivity and affordability remain a challenge, digital transformation plays a significant role in the continent's future, unlocking economic potential and driving inclusive growth.

However, this digital expansion comes with significant vulnerabilities. As connectivity increases without corresponding security measures, SMEs in the region have become particularly susceptible to cyber threats. The digital infrastructure gap that exists often means businesses are connecting to global networks without adequate cybersecurity awareness or protections in place. This security deficit has not gone unnoticed by cybercriminals, who increasingly view these emerging digital businesses as easy targets.

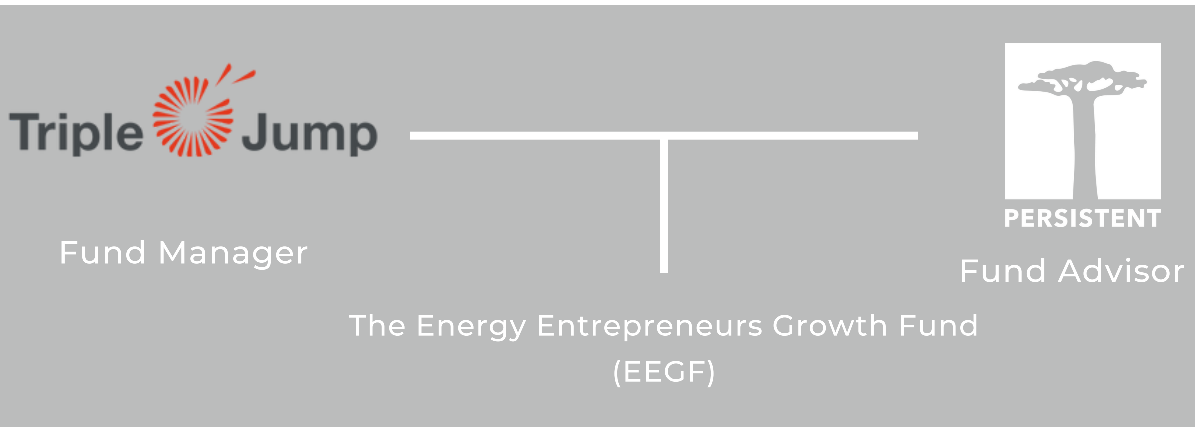
> ❞ *APPROXIMATELY 90% OF ORGANIZATIONS IN AFRICA OPERATE WITHOUT BASIC CYBERSECURITY PROTOCOLS* ❞

The lack of preparedness is stark — approximately 90% of organizations in Africa operate without basic cybersecurity protocols. This vulnerability contributes to significant economic losses, with cyber incidents costing African economies around 10% of their GDP which translates to billions of dollars annually.[2]

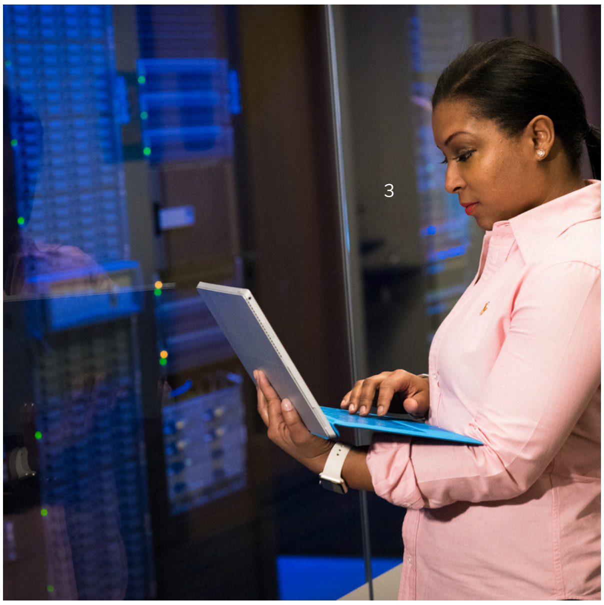
The Energy Entrepreneurs Growth Fund (EEGF), provides financing to early- and growth-stage companies operating in the access to energy ecosystem in Sub-Saharan Africa and India. EEGF's mission is to increase access to clean and affordable energy to off-grid families and underserved businesses, and contribute to the achievement of Sustainable Development Goal 7 by 2030. Persistent, as Africa's Climate Venture Builder and advisor to the EEGF, recognized that cybersecurity is one of essential components to look at when investing in the climate-focused SMEs. Together we have been equipping as many businesses in the African climate impact sector as possible with the knowledge and tools to safeguard their operations against cyberthreats as we view it as a crucial step in de-risking the investments in the sector.

As part of this mission, we conducted research on cybersecurity practices within the sector. We collaborated with industry stakeholders, ranging from African impact focused SMEs, to software and cybersecurity providers (in particular PaygOps, Upya and Practical Infosec) to assess the scale of the problem and develop practical interventions for the SMEs.

Thanks to EEGF's role in strengthening the access to energy ecosystem, we are publishing this white paper to share key findings from our research and lessons learned. Through EEGF's support, Persistent's custom-built cybersecurity toolkit has facilitated direct interventions that inform this work. Designed specifically to build awareness and preparedness, this toolkit equips organizations with practical strategies and tools to proactively strengthen their cybersecurity defenses. By fostering a deeper understanding of potential risks and enhancing readiness to address them, we aim to empower companies across the sector and beyond to prevent cybersecurity incidents before they occur and effectively mitigate their impact. Ultimately, this approach supports businesses in achieving a more secure, resilient, and sustainable digital future.
We hope that sharing our learnings will help kick-start a wider discussion in the industry and inspire both individual action and collaboration to strengthen cybersecurity across the board.



SUMMARY OF CONCLUSIONS



Africa’s digitalization is accelerating rapidly, driven by expanding internet penetration, a growing tech-savvy population, and significant infrastructure investments. This digital growth is unlocking economic potential and driving inclusive development, yet it also exposes businesses - especially SMEs - to increasing cyber threats. In our research for the EEGF, Persistent has homed in on the impact space through interviews with software providers and cybersecurity experts, surveys and hands-on work with companies from the EEGF portfolio.

Key research findings indicate that the region’s digital transformation, coupled with limited cybersecurity awareness and outdated or unevenly enforced regulatory frameworks, creates significant vulnerabilities. Common threats include phishing, weak-password breaches, and sophisticated tactics such as email spoofing and deceptive hardware. Notably, many SMEs underestimate their risk, assuming they are too small to attract cybercriminals, while larger organizations often shift the responsibility to external providers.

In response, EEGF and Persistent have developed a comprehensive Cybersecurity Toolkit. This toolkit, validated through industry surveys and collaborations with cybersecurity experts, offers practical interventions including staff training programs, automated self-assessments, in-depth security scans, policy templates, and incident response plans. The goal is to empower organizations - particularly those in the African climate impact sector - to proactively strengthen their cybersecurity posture. By fostering greater awareness, practical training, and systematic risk management, these efforts aim to mitigate potential losses, safeguard reputations, and support a more secure, resilient digital future for the region.

In order to significantly improve their cybersecurity posture, companies can start with implementing these five essential safeguards: regular cybersecurity training for staff, multifactor authentication (particularly for email accounts), strict need-to-know access controls, automated software updates, and well-defined incident response plans.

HOW SERIOUS ARE CYBERTHREATS IN THE AFRICAN CONTEXT?

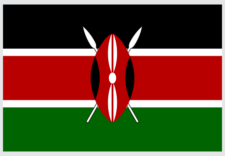
Cybersecurity often remains a low priority for many SMEs in Africa, largely due to limited financial resources. This is compounded by the misconception that small businesses, such as an off-grid solar distributor in rural Africa, are unlikely targets for cybercriminals. However, the reality is that any business or individual can become a victim of cyberattacks if it is not adequately prepared. Many cybercriminals rely on a "quantity over quality" approach, indiscriminately sending thousands of phishing messages in the hope that even a small fraction of recipients will fall for their schemes, making no organization too small or remote to be at risk. As a consequence, the cost of cybercrime in Africa surged from $0.5 billion in 2015 to $3 billion in 2020, and reached $4 billion annually in 2022, with South Africa, Nigeria, and Kenya experiencing the most significant losses ($570m, 500m and 36m respectively)[3]

$0.5 billion	$3 billion	$4 billion
Cybercrime losses in Africa (2015)	Cybercrime losses in Africa (2020)	Cybercrime losses in Africa (2022)

Top countries affected in 2022

South Africa
$570 Million

Nigeria
$500 Million



Kenya
$36 Million

As we learned through our survey, multiple companies reported cyberattacks, ranging from phishing and weak-password breaches to website takedowns and unauthorized data access. As we continued to work closely with EEGF portfolio companies to bolster their security, we encountered further examples, such as email spoofing—where attackers impersonated employees—and data theft through deceptive tools like fake USB-C charging cables.[4] These incidents highlight that successful attacks are far from abstract risks; they are concrete and frequent threats for businesses in our sector.

In addition to financial repercussions, such as ransom payments, cyberattacks can have other far-reaching consequences. Reputational damage is a major risk, leading not only to customer loss but also to reduced investor confidence, which can jeopardize crucial funding. Service interruptions caused by cyberattacks can result in lost revenue, frustrated customers, and significant resource investments to remediate the damage. Moreover, data breaches involving sensitive information, trade secrets, or intellectual property can severely undermine a company's competitive position. In short, cyberattacks can undermine a business to the point of its failure.

STATE OF AFFAIRS IN THE SECTOR - LEVEL OF PROTECTION AND DIRECTION OF THINKING ABOUT SECURITY

Africa faces unique cybersecurity challenges, with only 39 of 54 countries having comprehensive cybersecurity and data protection legislation.[5] Poor infrastructure, low awareness, and weak enforcement leave organizations - especially financial institutions including solar PayGo companies - vulnerable as digital transformation expands the threat landscape.

> *Only 39 of 54 countries have comprehensive cybersecurity and data protection legislation.*

To better understand cybersecurity perceptions, we conducted a survey with companies in the African climate impact sector, as well as interviews with two leading last mile management software providers, Upya and PaygOps (Masunga).

Throughout the interviews, both providers underlined their clients' disregard for cybersecurity — many were either unaware of the threats or assumed they were too small to be targeted. On the other hand, larger companies often enquire about cybersecurity insurance and expect security to be mainly the provider's responsibility. In addition, despite their efforts to promote good security practices, they often face resistance from clients who prioritize convenience.

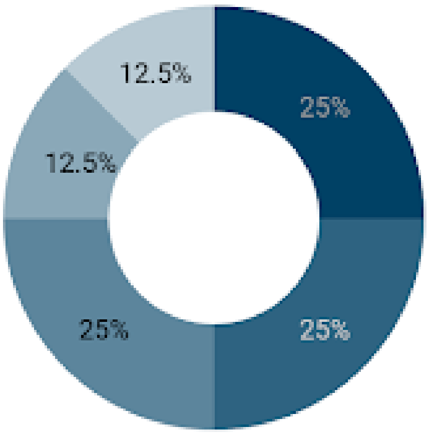
For instance, PaygOps attempted to restrict direct data downloads in favor of more secure data access routes via specialized analytics tools, but backlash from users led to the rollback of these security measures.

Benjamin David, CTO and Co-Founder at Masunga (the parent company of PaygOps) noted:

"While we design our tools with robust safety measures to store and protect data and ensure access is restricted to authorized users, cybersecurity is a shared responsibility. User awareness and safe digital practices are essential to complement our efforts, which is why education and training are so important."

Although staff training is one of the essential cybersecurity practices, our survey showed that such measures are often neglected, with only 30% of respondents having it in place. In addition, over half the respondents lacked confidence in senior executives' ability to make effective cybersecurity decisions, with many executives failing to prioritize the issue until after a security incident occurred. Companies that had experienced successful attacks were found to have implemented more measures afterward. In general, management viewed technology, including cybersecurity, as an expense rather than a priority, especially when funds were limited. A lack of knowledge was cited as a major reason for not taking cybersecurity seriously.

What are you most concerned about when it comes to IT security for the near future?



- ● Theft/loss of consumer data from consumer protection perspective
- ● Viruses and general loss of data
- ● Unauthorized access to data and threats through mobile devices
- ● Loss of company sensitive data for competitive reasons
- ● Secrete key and loan access management

Amongst the respondents with interest in cybersecurity, 70% acknowledged the importance of cybersecurity, and concerns about future IT security threats were widespread, with over 90% of respondents fearing potential adverse impacts, particularly data loss and customer data leaks. There was also an overreliance on technology alone to protect against threats, despite evidence showing that user mistakes—responsible for 88% of successful breaches[6]—are a major risk factor. Regular IT security training is critical to minimize such risks, helping employees identify phishing attempts and navigate online threats securely.

We collaborated with Practical Infosec, a cybersecurity advisory firm for purpose-driven organizations, to validate our findings and create practical tools to address the issue.

Founder Ashley Woodhall noted:

"***Impact SMEs in the region are highly successful at leveraging technology and often build their own tailored systems. The disadvantage to this approach is a huge reliance on technology which often misses crucial security protection. When we highlighted key security risks to these management teams, they were quick to act, protecting their technology and organisations.***"

Overall, our findings indicate that there is insufficient understanding of the necessary cybersecurity measures and their implementation, resulting in a lack of effective action on the ground. Increasing awareness and understanding of how cyberthreats are executed, emphasizing training, and prioritizing cybersecurity are essential to provide Africa's businesses with the tools they need to address unique challenges and protect their rapidly evolving digital landscapes.

ENHANCING CYBERSECURITY THROUGH A SYSTEMATIC APPROACH: THE CYBERSECURITY TOOLKIT

Our research into cybersecurity challenges in the sector has provided valuable insights into the scale of the problem, leading us to develop a **Cybersecurity Toolkit**. It was initially created to mitigate risks across the EEGF portfolio but our goal is to expand its reach. This Toolkit is designed to systematically identify and address vulnerabilities in cybersecurity frameworks. It consists of a suite of practical, actionable tools that can either be directly used by companies, provided they have internal capacity to do so, or deployed collaboratively by the **Persistent Tech Team**, or other third-party providers in partnership with each organization

The Cybersecurity Toolkit includes:

- **Staff training deck and quiz**: A structured program designed to build foundational cybersecurity awareness among employees.

- **Automated cybersecurity self-assessment tool**: A quick, structured evaluation that enables companies to assess their security posture and receive an initial security score.

- **In-depth cybersecurity scan**: A more detailed analysis conducted via direct engagement with a qualified professional to identify and address significant vulnerabilities.

- **Policy and incident response plan templates**: Ready-to-use templates for security policies and incident response plans, helping companies formalize their approach to security.

- **Regulatory compliance support**: Guidance on local cybersecurity regulations and best practices to ensure adherence.

- **Hands-on implementation support**: Direct assistance in executing cybersecurity improvements, such as cloud architecture redesign or **DMARC** implementation.

EMPOWERING EMPLOYEES: THE ROLE OF CYBERSECURITY TRAINING

Recognizing the **pivotal role of employee awareness**, our cybersecurity strategy places strong emphasis on staff training. Our approach begins by **identifying and equipping trainers** within the organization - individuals who will champion security awareness efforts and train their colleagues, ideally in-person. These trainers are provided with an enhanced version of our training program, enabling them to confidently educate others, even in companies without dedicated IT personnel.To further support trainers, we are developing a custom AI chatbot that will serve as an on-demand resource, assisting with any questions or uncertainties that arise during training sessions.

Additionally, companies receive a core cybersecurity training deck covering essential topics such as:

- Recognizing and preventing phishing attacks
- Creating and managing strong passwords
- Enforcing **multi-factor authentication (MFA)**
- Securing devices and networks in public spaces
- Safe browsing practices
- Implementing foundational cybersecurity measures

FROM ASSESSMENT TO ACTION: A DATA-DRIVEN APPROACH

A cornerstone of our methodology is the **Cybersecurity Self-Assessment Tool**, a short survey that companies complete to evaluate their security practices. The survey results generate an automated security score, offering a preliminary glimpse into a company’s cybersecurity posture. AI-driven recommendations are reviewed by Persistent staff before being shared and discussed with the company. When substantial vulnerabilities are identified, we follow up with an **in-depth cybersecurity scan**, which involves further discussions and targeted interventions to strengthen security measures.

By aggregating data from multiple assessments, we gain a **comprehensive overview** of cybersecurity trends across the portfolio. This enables us to pinpoint common challenges and tailor our support accordingly. The aggregated data is solely shared on a need-to-know basis. Company specific data is kept confidential and only used for the intervention in question

STRENGTHENING SECURITY POLICIES AND INCIDENT PREPAREDNESS

As part of our **Cybersecurity Toolkit**, companies receive **security policy templates** and **incident response plan frameworks** to streamline their security protocols. These resources play a crucial role in establishing clear security guidelines, ensuring companies can preemptively mitigate threats and respond effectively to breaches. A well-defined security policy provides employees with structured procedures to follow, reducing human error and improving compliance with industry standards. Incident response plans, on the other hand, enable organizations to react swiftly and efficiently to security incidents, minimizing operational disruption, financial losses, and reputational damage. By equipping companies with these essential tools, we help them foster a proactive security culture and build resilience against evolving cyberthreats.

MEASURABLE IMPACT AND LESSONS LEARNED

To date, the EEGF has successfully implemented components of the Cybersecurity Toolkit with 13 companies, yielding consistently positive feedback. Companies report a greater sense of security, having addressed critical vulnerabilities and observed **measurable improvements** in their security scores post-implementation.

One of the most valuable insights from our work is that **small, non-technical interventions**—such as enforcing **multi-factor authentication (MFA)** or integrating **regular cybersecurity awareness training**—often deliver **greater security benefits** than complex technical patches. By simplifying cybersecurity and making it more accessible, we empower companies to take proactive, practical steps toward robust digital resilience.

INDUSTRY-WIDE RECOMMENDATIONS FOR CYBERSECURITY IMPROVEMENT

Based on our experience implementing the **Cybersecurity Toolkit** within the EEGF portfolio, we have identified key measures that can significantly enhance cybersecurity across the industry. By adopting these straightforward yet impactful improvements, companies can strengthen their security posture and better protect themselves against cyberthreats.

PRIORITIZING EMPLOYEE TRAINING AND AWARENESS

User errors, such as falling for phishing and social engineering attacks or using weak or reused passwords, remain one of the primary causes of cybersecurity breaches. To mitigate this risk, we strongly recommend that companies implement **regular cybersecurity training programs**, ideally on an annual basis. Platforms such as **KnowBe4** provide structured training solutions, but an even more effective approach is to establish **internal security champions** within the organization. In-person training sessions led by these champions are more effective than platform-based solutions because they foster direct engagement, allow for real-time questions and discussions, and encourage a more interactive learning environment. Employees are more likely to retain knowledge when they can relate it to their specific work context and discuss real-world scenarios with a familiar colleague. Additionally, having an internal security champion creates a point of contact within the organization whom employees can approach with concerns or questions, ensuring that cybersecurity remains an ongoing conversation rather than a one-time training event.

ENFORCING MULTI-FACTOR AUTHENTICATION (MFA)

One of the simplest yet most effective security measures is the **enforcement of MFA**, particularly for critical applications such as email. MFA provides an additional layer of defense against compromised passwords, ensuring that unauthorized users cannot gain access even if login credentials are stolen. Email security should be a top priority, as compromised email accounts can be leveraged to reset and access other linked accounts. Following this up with the implementation of **Single Sign-On (SSO)** solutions can further streamline authentication processes, reducing the need for multiple complex passwords while maintaining security.

IMPLEMENTING PASSWORD MANAGEMENT BEST PRACTICES

For companies with sufficient budgets, a **company-wide password manager** can be an excellent investment. Password managers encourage the use of strong, unique passwords while also providing management teams with insights into password strength and usage across the organization. However, for companies with extensive networks of agents or external collaborators where a password manager may not be financially feasible, alternative measures include:

- Educating employees on creating **strong but memorable passwords**.
- Enforcing **least privilege access**, ensuring that users only have access to the applications and data necessary for their roles.

ENSURING SYSTEM AND SOFTWARE UPDATES

Keeping systems up to date is a **non-negotiable aspect of cybersecurity**. Companies should ensure that all employees regularly update their devices and applications, as software updates often include patches for known vulnerabilities. Where possible, **automated updates** should be enabled on company-owned hardware to minimize reliance on manual interventions. Organizations that develop their own software must take additional responsibility for updating applications, servers, and software dependencies to prevent security gaps from being exploited by attackers.

MITIGATING EMAIL SPOOFING WITH DMARC IMPLEMENTATION

Email spoofing remains a major cybersecurity challenge in many sectors. This form of cyber deception involves forging the sender's address in an email to make it appear as though it was sent from a legitimate source, often tricking recipients into divulging sensitive information or taking harmful actions. Spoofed emails can be used for phishing attacks, spreading malware, or conducting financial fraud.

Implementing **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** helps prevent unauthorized senders from impersonating company domains.

By authenticating email sources and blocking messages from unapproved senders, DMARC significantly reduces phishing risks and enhances overall email security. Organizations that fail to address email spoofing risk financial losses, data breaches, and damage to their reputation, making DMARC implementation a crucial security measure.

DEVELOPING AND TESTING INCIDENT RESPONSE PLANS

Cybersecurity preparedness is just as important as prevention. A well-structured **incident response plan** can drastically reduce recovery time and financial losses in the event of a cyberattack. By proactively outlining recovery procedures, communication protocols, and the roles of responsible personnel, companies can ensure a swift and effective response. Incident response plans should also account for **legal, regulatory, and contractual obligations**, ensuring compliance with applicable cybersecurity frameworks.

CONCLUSION

Implementing these key cybersecurity measures can help companies in the African impact sector and beyond level up their cybersecurity posture with minimal effort and investment.

Throughout our research, we have learned that awareness around cybersecurity is still lacking in the sector. Since awareness is the key building block for forming a strong foundation for secure organizations, we hope this white paper will kick-start discussions on building a more resilient sector.

We continue rolling out the Cybersecurity Toolkit as part of our Venture Building activities, assisting companies in putting the recommended measures into practice. By fostering cybersecurity awareness and supporting practical implementations, we aim to contribute to a more secure and resilient impact sector. More importantly, robust cybersecurity practices protect organizations from financial losses, reputational harm, and operational disruptions. In the impact sector, where businesses focus on social and environmental benefits, safeguarding sensitive business and customer data is particularly critical. Cyber breaches not only threaten financial stability but also risk undermining an organization’s core mission and the communities it serves.

NOTES

This research project was funded by the EEGF.

We would like to give special thanks to Practical Infosec, PaygOps, and Upya for their participation in this research. Their respective contributions to collecting data, shaping a more complete picture of how cybersecurity is treated in the African impact space and in shaping the practical tools have been invaluable.

- **Practical Infosec** provides practical security advice for purpose-led organizations.
- **PaygOps** provides flexible, modular software solutions that streamline operations for essential service providers - from leads and contract management to payments, ticketing, and inventory - improving efficiency and enhancing customer experience.
- **Upya** offers a highly scalable and adaptable platform to enable distributors of any products and services to efficiently manage operations, teams, and customers in complex environments

REFERENCES

1) Our thanks to the many commentators who reviewed a draft of this article and provided their valuable feedback.
2) National Cybersecurity and cybercrime policies in Africa
3) https://african.business/2023/02/technology-information/africas-cybersecurity-threat#
4) A hack consisting of leaving altered USB-C charging cables in public places such as charging stations. These cables can be hacked to inject malicious code, communicate activity to the attacker or even give the hacker full remote access to the device.
5) Africa Cyber Security Outlook KPMG International
6) https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error

ABOUT PERSISTENT

Persistent is Africa's Climate Venture Builder. For over a decade, Persistent has been a leader in developing and investing in climate-focused businesses that are part of the Energy Transition. Our investing and company building in solar energy, e-mobility, and energy efficiency have positively impacted over 10.5 million people, avoided over 2.1 million tons of CO2e, created 21,400 jobs, and provided clean energy services to over 15,000 SMEs. Our approach combines equity investment with human capital support to early-stage, impact-driven companies, accelerating their pathways to scale and profitability. While we continue to focus on supporting the Energy Transition, we are beginning to invest in climate-focused businesses that are part of the Resource Transition and the Agricultural Transition. Persistent is dedicated to promoting a sustainable future while delivering exceptional returns to our investors. We are currently raising the Persistent Africa Climate Venture Builder Fund to increase our level of investing and company building.

ABOUT TRIPLE JUMP

Triple Jump is a Dutch impact-focused investment manager dedicated to creating positive change in emerging markets. Managing and advising on funds that generate both financial returns and social impact, Triple Jump operates across five key development themes: financial inclusion, SME finance, affordable housing, access to clean energy, and climate and nature. With a global presence and local expertise, the firm manages over €1 billion in assets, supporting projects that contribute to sustainable and inclusive financial sectors. Triple Jump has offices in Amsterdam, Nairobi, Lima, Mexico City, Tbilisi, and Bangkok.

ABOUT THE ENERGY ENTREPRENEURE GROWTH FUND

The Energy Entrepreneurs Growth Fund (EEGF) was initially led by Shell Foundation, in collaboration with FMO, the Dutch entrepreneurial development bank. Over time, it gained steadfast support from reputed development institutions like FinDev Canada, the Development Bank or Austria (OeEB), The Nordic Development Fund (NDF), the United States International Development Finance Corporation (DFC), and the African Development Bank (AfDB). Managed by Triple Jump and advised by Persistent, EEGF offers customized mezzanine, equity, and debt investments, along with technical assistance, to early and growth-stage companies in Sub-Saharan Africa's energy sector. EEGF expands last-mile energy access in underserved regions of Sub-Saharan Africa and India, driving socio-economic development and a just energy transition. By leveraging diverse capital, primarily risk-taking debt like mezzanine, it scales high-potential energy enterprises, fostering sustainable growth and improved livelihoods.