CYBER1 illustrates a strong start to 2023 through organic growth and acquisitions

	2023	2022
Revenue		
Q1 2023	**€ 13,370k**	**€ 9,487k**
Gross Margin		
Q1 2023	**€ 3,113k**	**€ 1,892k**
EBITDA		
Q1 2023	**€ 392k**	**- € 564k**

Group Performance

Group revenue increased significantly (41%) year on year from €9,487k in Q1 2022 to €13,370k in Q1 of 2023. This has been achieved through our own organic growth with additional customer acquisition and development of new technologies, coupled with the groups expansion and investment spend in 2022.

Gross margin for Q1 is 3% up on the prior year, mainly attributable to the refreshed group strategy of the establishment and utilisation of the Next-Gen Security Operating Centre (SOC) offering, combined with innovative vendor partnerships to increase the company's margin.

Operating Expenditure for Q1 has marginally increased by €241k compared to 2022, an increase of 9%. The increase reflects the operating costs of the acquisitions business included in the current year not included in the comparative period. Overall the combination of increased revenues, improved margin and stricter cost control measures, the business has turned a positive EBITDA result of € 392k compared to a loss in Q1 2022 of € 564k.

Material investment was made last year for the implementation of the company's strategy which is proving to be successful and on track with the company's objectives. CYBER1 continues to gain accreditations and build further infrastructure and capabilities for its Next-Gen SOC, adding a new recurring revenue business model and ensuring a wider commercial scope for engagements in key target regions. CYBER1 has provided additional resources for technical capabilities across the Group, to facilitate newly acquired commercial territories for key vendors.

Our business at a glance

CYBER1 is a multi-product and multi-jurisdictional leader in cyber security advisory and solutions. We are uniquely placed to help customers achieve cyber resilience and thus, safeguard reputation and value. Providing innovative and cost-effective services and solutions requires experienced staff. CYBER1 Solutions employs a significant number of security-certified technical consultants, providing superior knowledge & comprehensive expertise. We have highly skilled and experienced technical teams located in our regional offices in Johannesburg, Cape Town, Nairobi, Dubai, and Europe

CYBER1 has three main strategic segments:

TRINEXIA is the trusted Cyber Security, Digital Forensics, Identity and access management and breach and attack simulation value added distributor of leading solutions across Europe, Middle East, Africa, Southern Africa, and India. We are consistently and successfully adding guidance and expertise to our partner community, where we design and deliver solutions that are customised to achieve the required results, whilst being renowned for our people, partnerships, and performance.

CYBER1 SOLUTIONS - Our solutions deliver information security; IT risk management; fraud detection; DevSecOps; as well as a full range of managed services. We also provide bespoke security services across the spectrum, with a portfolio that ranges from the formulation of our customers' security strategies to the daily operation of end-point security solutions. To do this, we partner with world-leading security vendors to deliver cutting-edge technologies augmented by our wide range of professional services.

C1 SOC – Our Next-Gen security operations centre (SOC) – is equipped with the latest technologies and expertise that can help bolster the security posture of any organisation and is currently undergoing an ISO certification process. Building and maintaining your own SOC can be prohibitively expensive, and hard to manage without the right resources. Outsourcing this function gives your business a solution that puts a team of Cyber Security experts at your disposal 24/7 and won't break the bank.

Having highly skilled analysts on board to detect advanced threats and offer advanced managed detection and response services will enable your business to identify, respond to and mitigate these threats before they become a problem.

Beyond the Quarter and other news

CYBER1 announced that its solution division (CYBER1 Solutions) has expanded its European presence, with the appointment of Hilbert Long as the General Manager for the region in line with the strategic growth objectives. The company's European commercial office will be based out of London and with staff across EMEA. The business aims to grow its footprint in the region by expanding its set of cyber security services to current and future customers.

"Our strategy is to grow the entity to become a self-sustaining fully-fledged business within the European market," says Hilbert Long. "We aim to replicate the strong businesses we have built in South Africa, as well as East and West Africa, using our expertise and knowledge to build another CYBER1 Solutions in the region."

CYBER1 announced a partnership with 9th Bit Consulting, a leading provider of Information Technology Integration, Middleware, SOA, Microservices / API's, DevSecOps, Security and related Solutions and Services.

Robert Brown, Group President & Executive Director of CYBER1 commented that "I am delighted to establish this new relationship and agreement with 9th Bit Consulting. We believe there are a number of synergistic opportunities in the DevSecOps space and the convergence of security practices we see that are required with our customers.

We believe that our joint approach on larger customer opportunities (both new and existing) will greatly benefit from this partnership. I am excited to collaborate further with Barry De Waal and Gerhard Van Niekerk (owners of 9th Bit Consulting) and the rest of the 9th Bit team, in developing our mutual strategic engagement for the future.

From the desk of the President

Dear Shareholders,

Global instability, financial unrest and increased political polarisation has led to increased awareness of threats and actual attacks on digital systems globally. The cyber security service offerings become more and more central in any operational business around the world. With more than 20 years' experience, CYBER1 is extremely well positioned in this rapidly development market.

Following the completion of several projects and the implementation of a new corporate strategy, it is pleasing to announce a profit for the opening quarter of 2023. This has derived from increase headline growth, improved margins and easing of initial one-off investments. Building on the back of a year of expansion both organically and through acquisitions, we are starting to see the collaborative opportunities within the three business units of Value-Added Distributions, Advisory and Solutions and our Next-Gen SOC.

The two latest entities, TRINEXIA South Africa and TRINEXIA Africa continue to integrate into the CYBER1 family. With a combined force in the Middle East in TRINEXIA DMCC, we have exponentiality expanded our capabilities and commercial footprint, where our valued vendors can better realise our scale of operations extend our relationships with the leading partners in the regions.

Our results for the quarter saw a significant profitability improvement year over year. Most importantly however, is that we did not grow from the inclusions of acquisitions alone, with year over year growth from business reported in Q1 of last year increasing their revenue by 9%. Significant planning was undertaken between the board of directors and executive management in 2022 and it is pleasing to see some of those ideas starting to equate to improvements around the business.

Our Next-Gen Security Operations Centre continues to expand its customer base and unique partnerships. We aim not only to work with individual entities but be able to provide an array of white labelling capabilities with organisations wishing to deliver this service. We are also progressing well with several industry standard accreditations, so that our services can be delivered globally with the best practises and capabilities. Through our highly accredited technical team monitoring the SOC twenty-four hours a day, we are continuously able to detect and remediate against the latest threats.

The company outlined four key growth objectives that will underpin the planned growth of the business until 2025.

With our aim to expand into target territories, we have made progress with working with our leading vendors to assess our go to market approach. With our new acquisition inclusions across Africa, our territory scope has given us a strong platform in which to build a sound commercial footprint. Most notably, our announcement beyond the quarter of extending our footprint into Europe will provide new greater opportunities for CYBER1 where our company is listed.

With our SOC offering, we have onboarded new customers, increasing the various industries that we supply threat intelligence and monitoring services to. We are planning further cross selling into Europe, as well as with some exciting partnerships we are building in new markets for the Group.

We are continuously engaging with the latest innovative technologies on the market. Our executives attended the RSA conference in San Francisco in April, discussing with the key leaders in the industry on the emerging threat trends, new technologies surrounding artificial intelligence, as well as opportunities for the company.

Our expansion into the DevSecOps space continues to develop, as we work with key stakeholders and partners on formalising our overall approach. With our existing sales infrastructure and knowledge of complementing technologies, we are well positioned to harness this latest area of development.

With our growth objectives progressing, we believe that these areas will ensure the company is at the forefront of cyber security prevention, detection, and remediation.

Stockholm, 23 May 2023
Robert Brown
Group President and Executive Director

Key Financial Ratios

	Jan - Mar Q1 2023	Jan - Mar Q1 2022	Jan - Dec 2022
	€'000	€'000	€'000
Group Income	13 370	9 487	46 833
Group Gross Margin	3 113	1 892	9 313
Group Gross Margin percentage	23%	20%	20%
Cash flow from operations	601	136	-4 591
Operating Margin	289	-691	-3 638
Operating Margin percentage	2%	-7%	-8%
Result after taxes	206	-689	-3 866
Earnings per share	0.0019	-0.0062	-0.0031

Business Overview

Market Update

During the start of 2023, emerging technologies such as artificial intelligence/machine learning, 5G, IoT, and quantum have already had a significant impact on anything that is connected to the internet.

However, the introduction of these potentially disruptive technologies has brought with it implications on cyber security and the challenges of keeping data secure. There is a growing concern about the potential misuse of generative artificial intelligence, which can leverage powerful tools such as ChatGPT-powered code and ai/machine learning to enhance social engineering capabilities and identify target vulnerabilities for hackers. These emerging tech trends and statistics are already painting a clear picture for 2023.

As data production and storage volumes continue to increase, and internet connectivity expands rapidly across the globe, the attack surface has become more exploitable with various gaps and vulnerabilities for criminal and nation-state hackers to exploit. Unfortunately, attackers have been taking full advantage of the evolving environment. In fact, global cyber-attacks have already risen by 7% in Q1 of 2023. According to Check Point's latest research report, weekly cyber-attacks have increased worldwide, with each organization facing an average of 1248 attacks per week. Shockingly, the education and research sector experienced the highest number of attacks, with an average of 2507 per organization per week, which is a 15% increase compared to Q1 2022.

Opportunities for Cyber Security

For organizations looking to mitigate and protect against these trends, there are several opportunities to harness solutions that are posed by cyber-attackers.

The use of Artificial Intelligence and Machine Learning: AI and Machine Learning can be deployed to identify patterns of abnormal activity that could indicate the presence of a cyber-attack. This could enable organizations to detect and respond to threats more quickly and accurately. The C1 SOC uses the latest threat hunting and intelligence to detect against potential exploits.

Cloud-based security solutions can help to secure data and applications that are hosted in the cloud. This could include solutions such as cloud access security brokers (CASBs), which can provide visibility and control over data that is stored in the cloud. CYBER1 partners with leading CASB provider Palo Alto Networks.

Network security technologies such as virtual private networks (VPNs), network firewalls, and intrusion detection systems can be used to secure networks from cyber-attacks. This could help to prevent unauthorized access to sensitive data and systems. CYBER1 collaborates with innovative vendors such as Darktrace, Check Point and Palo Alto Networks in protecting networks from the latest threats.

One of the most effective ways to mitigate the risks posed by cyber-attacks is to provide employees with cybersecurity awareness training. This could help to raise awareness of the risks of cyber-attacks and educate employees on best practices for staying safe online. CYBER1 partners with KnowBe4 to help organisations enable their workforce to mitigate against an array of social engineering attacks.

By leveraging these cyber security technologies, organisations can significantly reduce the risks posed by cyber-attacks and protect their sensitive data and systems from unauthorized access, theft, and other forms of cybercrime.

Contacts

About CYBER1 (Nasdaq First North Growth Market: CYB1.ST)

CYBER1 is engaged in providing cyber resilience solutions and conducts its operations through presences in Sweden, Kenya, South Africa, United Arab Emirates, and the UK. Listed on Nasdaq First North Growth Market (Nasdaq: CYB1.ST), the Group delivers services and technology licenses to enhance clients' protections against unwanted intrusions, to provide and enhance cyber resilience and to prevent various forms of information theft. For further information, please visit www.cyber1.com/investors.

Outlook and Financial Information

Through the strategic changes implemented throughout 2022, the company has seen greater collaboration across the business units within the three operating segments of the business. Demonstration of our global footprint with the newly acquired entities will greatly aid the company in negotiation stronger margins, larger scaled projects and additional professional services that can be delivered across our scope. Through its managed services offering, CYBER1 is aiming to increase its overall reoccurring revenue from greater service billing via the Next-Gen SOC. This will be complemented by the business that is secured over a multiyear partnership with customers yet to be delivered. Combining both components with new enterprise commercial deals will be a key objective for the group, to ensure consistent profitability.

Business trend January 2023 to March 2023

Through the planned investments made in 2022, CYBER1 saw both acquisitive and organic growth, compared to Q1 2022. CYBER1 continues to drive its strategic growth objectives to make our approach as efficient as possible, whilst realising sustainable long-term prosperity.

We do anticipate this growth trend to continue as the company maintains the focus to the more niche technical products and the proliferation of its Next-Gen SOC services, whilst developing its traditional business offering.

The group continues to streamline expenses and improve profitability, ensuring financial sustainability and long-term success. Q1 2023 operating costs have increased by € 241k (9%) from the same period last year. The group is successfully implementing cohesive cost management protocols enabling the business to meet its obligations as a listed company on Nasdaq First North Grow Market. The group is optimistic that it can build appropriate cash flows within the business to be utilised for the benefit of future commercial endeavours.

CYBER1 will continue to make investments in its managed service offering, skilled resources, and cloud platform to aid the long-term success of the group.

Development of revenue and results

The remarked revenue growth in the first quarter is directly attributable to the planned group strategy which the group started implementing in 2022. The renewed focus on niche technologies has seen a growth in the margin of 3% to 23% (2022: 20%).

Earnings before interest and taxes on continuing operations (EBIT) turned a profit this year of € 289k from a loss in the prior year of € 691k.

As a result of the positive results this quarter, the group expects to see improved cash inflows in Q2 2023. Keeping the Parent Company lean and efficient and focusing on global operating efficiencies continues to be a main focus area of the Board and the executive team.

Outlook

CYBER1 maintains itself at the cutting edge of mitigations against threats and vulnerabilities in order to effectively protect its clients' data and systems. To achieve this, CYBER1 recommends customers take a proactive approach towards mitigating the latest threats.

CYBER1 approach recommends ensuring systems are regularly checked for vulnerabilities, and that all necessary updates are installed promptly.

To enhance its threat detection capabilities, our approach for resiliency revolves around investing in advanced tools and technologies such as machine learning and artificial intelligence type technologies. This will enable organisations to detect and respond to potential threats in real-time, before they can cause significant damage.

Adopting a multi-layered security approach, utilising a combination of technologies such as firewalls, intrusion detection and prevention systems, and data encryption will improve an overall security posture. This approach helps to ensure that even if one layer of security is breached, there are other measures in place to prevent attackers from gaining access to sensitive data.

Finally, providing regular security training for all employees and stakeholders ensures that staff are aware of the latest threats and how to respond to them. This will help to create a culture of security within the organization and ensure that everyone is working together to mitigate potential threats.

By taking these steps, CYBER1 can provide its clients with the highest level of protection against the latest cyber threats, while also maintaining its position as a leader in the cyber security industry.

Risk and opportunity report

CYBER1's risk policy is based on a business strategy, which focuses on safeguarding the Group's existence and sustainably increasing its value. Entrepreneurial activity is always forward-looking and therefore subject to certain risks. Identifying risks, understanding them, as well as assessing and reducing them systematically are the responsibility of the Managing Board and a key task for all managers.

CYBER1 is subject to various risks on account of its international business activity. Provided that they are consistent with the legal and ethical principles of entrepreneurial activity and are well balanced by the opportunities they present; these risks are classified as acceptable. Opportunity and risk management at CYBER1 is closely linked by Group-wide planning and monitoring systems.

Opportunities are recorded in the annual operational plan and followed up as part of monthly financial reporting. Operational management in each country and the central Group departments are directly responsible for identifying and observing opportunities at an early stage.

Risks and opportunities that may have a significant impact on our financial position and performance in the 2022 financial year and in the foreseeable future are described in detail in the 2022 Annual Report

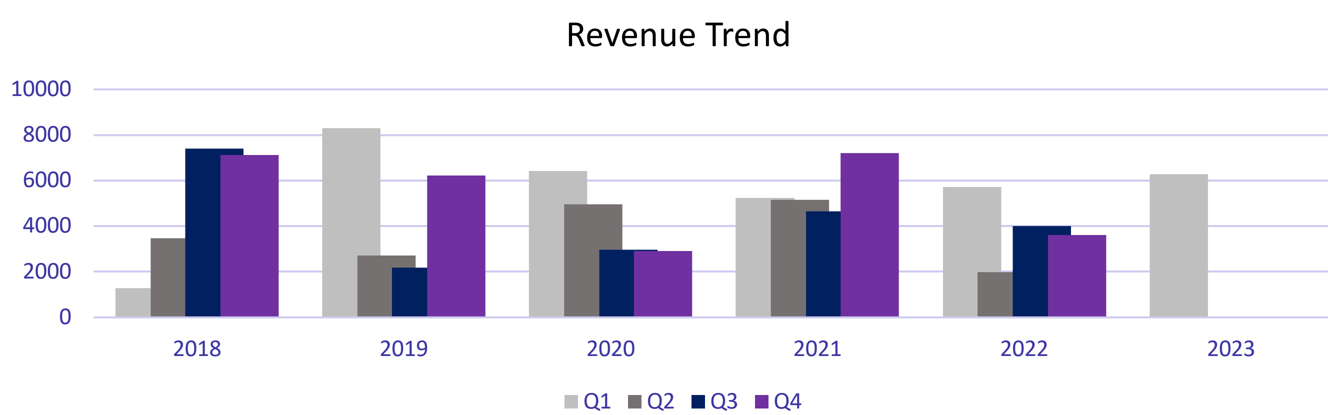
	Southern Africa
Revenue Q1	€ 6,285,163
Gross Margin	€ 1,271,275
EBITDA Q1	€ 145,563

CYBER1 Solutions Southern Africa

CYBER1 Solutions Southern Africa has started Q1 positively closing €6,285k of revenue, which is a 90% year over year increase compared to Q1 2022. The business unit has been able to convert the partnership engagement with some of the latest technology offerings and implement these within some of their longstanding clients. C1 Solutions SA has started to see the benefits of the coordinated strategic approach at the end of 2022, with a focus on further developing its core offering with established vendors, whilst assessing where niche vendors can add a point of difference within security infrastructures.

The improved margins and profitability for the organization has been underpinned by the increased delivery of services, including the Security Operating Centre offering we now have available across the group. With a greater alignment with our vendors, the company is well positioned to maximise the opportunities present within Africa.

Notable deals for the quarter included solutions for a large energy company, additional new business within an African Government department and upselling sales realised within a key strategic financial service institution within South Africa.



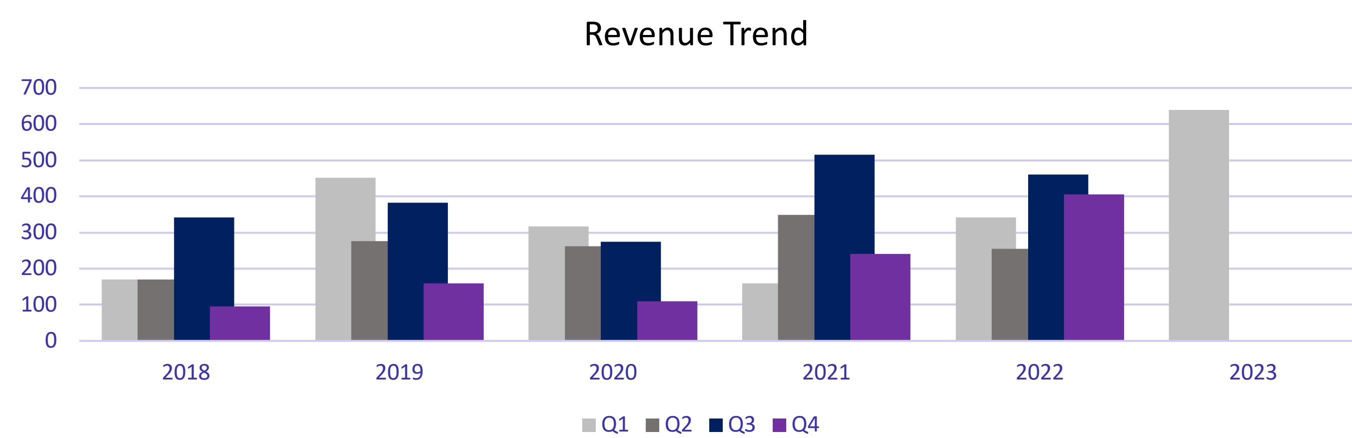
	East and West Africa
Revenue Q1	€ 640,856
Gross Margin	€ 180,004
EBITDA Q1	€ 28,773

CYBER1 Solutions Kenya

CYBER1 Solutions East & West Africa, based in Nairobi Kenya, recorded €640k for the first quarter of the financial year, which is an 88% year over year increased versus Q1 of 2022. The subsidiary has worked extensively at the backend to develop a strong pipeline for 2023. This has returned a significant 46% of new enterprise business for the quarter.

The company has continued to evolve its operational approach, which has led to an innovative approach to its professional service delivery to its key clients. Several marketing activities and events predominately around thought leadership and attending the Banking Summit in East Africa, to drive positive change within the region around best practices and approaches to the latest threats.

The company continues to drive its strategic growth initiatives, including the closure of key public sector accounts, to provide strong references for expansion, as well as improve training and accreditation skills on key vendors for the entity. Key wins for the quarter included a large new enterprise solution for a large-scale energy provision within Eastern Africa, as well as cyber security provisions for a government revenue authority within Africa.



	EMEA
Revenue Q1	€ 532,207
Gross Margin	€ 121,487
EBITDA Q1	€ 16,885

CYBER1 Solutions EMEA

As announced during 2023, CYBER1 Solutions, a cyber security services company with 26 years of industry expertise, has announced the expansion of its European presence and the appointment of Hilbert Long as General Manager for the region, in line with its EMEA (Europe, Middle East and Africa) expansion plans.

The entity has started positively, with revenues of €532k for the first quarter of their operations. The management brings extensive experience of sales creation and delivery across several leading cyber security vendors. New technologies onboarded will positively impact not just the European region, but also within the Middle East and Africa, where new partnerships can be cross sold into existing client's infrastructures where value add can be realised.

The company's European office will be based in London with staff across the EMEA region. The business aims to grow its footprint in the region by expanding the cyber security services provided by its established businesses in Kenya and South Africa into EMEA.

TRINEXIA

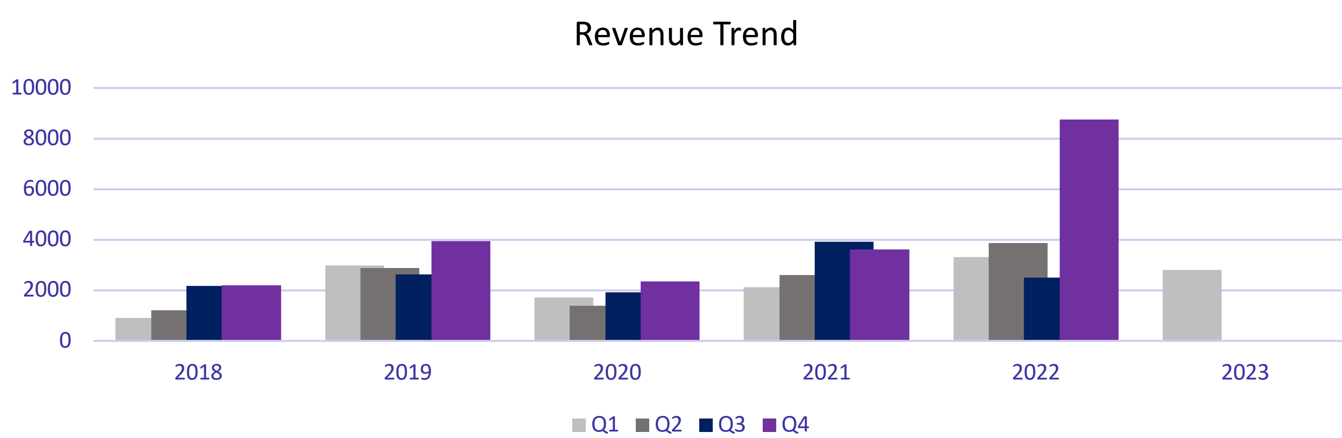
Middle East and India	
Revenue Q1	€ 2,808,281
Gross Margin	€ 728,217
EBITDA Q1	€ 68,254

TRINEXIA Middle East

TRINEXIA Middle East has started strongly for 2023, by implementing a strong new sales approach to its business offering, record €2,808k and 75% of new enterprise deals. Through its collaborative partnerships with resellers in the region, the entity continues to drive the latest cyber security and forensics solutions across the Middle East and India.

Company representatives of TRINEXIA attended a few key events, including GISEC 2023, the World Police Summit, as well as the start of the TRINEXIA Roadshow. The company will travel across the region to promote the latest vendors to combat against the latest evolving threats.

Notable wins for the quarter include a leading financial institution in the Middle East, as well as solutions for armed forces, police services and other government institutions across the regions.



	Southern Africa
Revenue Q1	€ 1,502,852
Gross Margin	€ 281,031
EBITDA Q1	€ 29,002

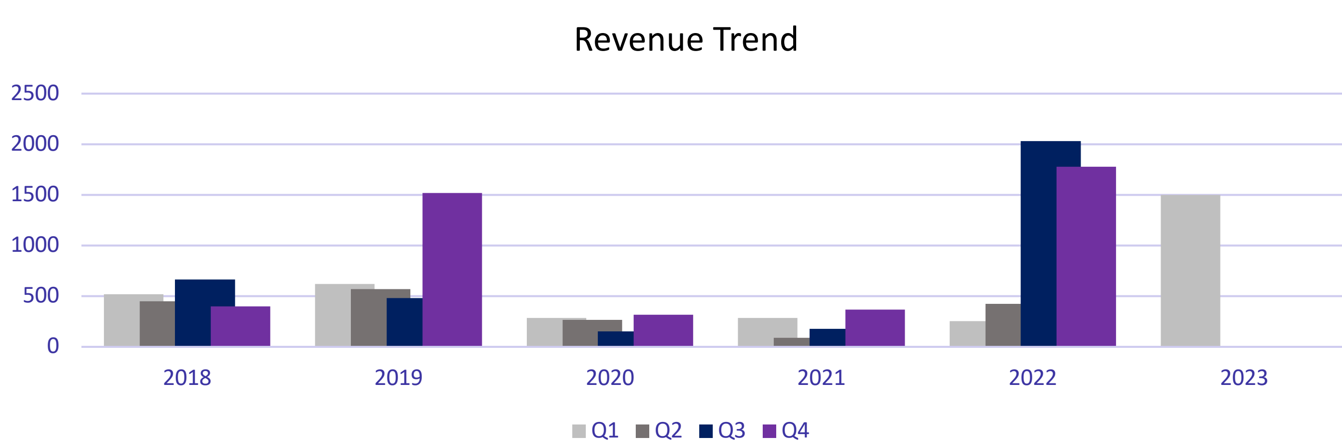
TRINEXIA Southern Africa

TRINEXIA Southern Africa, formerly known as Cyber Security South Africa (CSSA) has started the year positively, recording €1,502k of revenue for the quarter, its most successful first quarter to date since its formation.

The business has managed to grow its healthy year-on-year growth through expansion of its existing target customer segments, through its proven delivery. Greater collaboration across the Group with other subsidiaries into 2023, will further augment the capabilities of TRINEXIA South Africa.

TRINEXIA South Africa was able to attend CISO Africa, where new opportunities were realised whilst discussing with key stakeholders on budling a robust and resilient security community for African businesses.

Notable deals for the quarter included a leading national retailer in South Africa, solutions for one of Africa's largest financial service institutions and a key government department within Southern Africa.



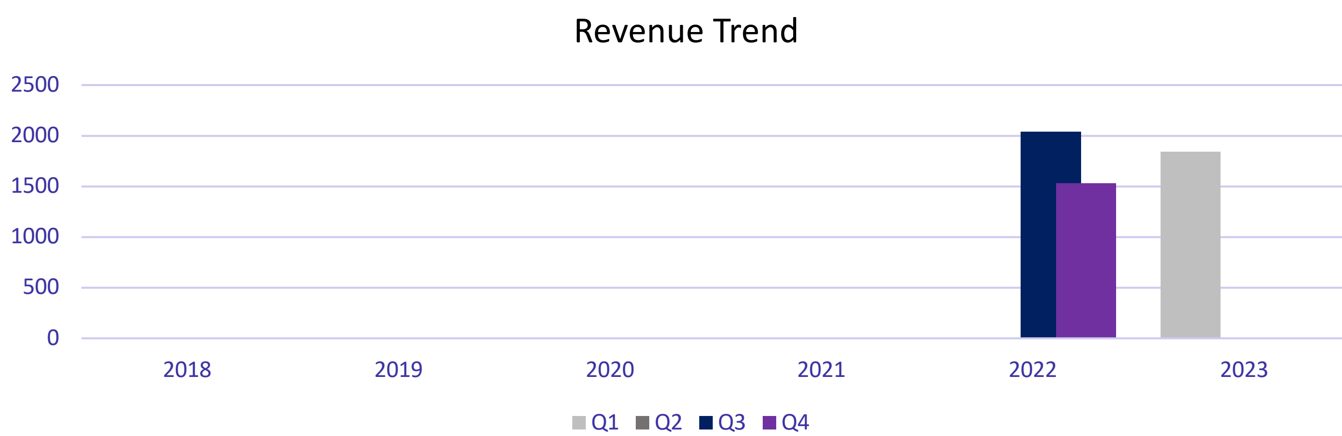
	Africa
Revenue Q1	€ 1,839,558
Gross Margin	€ 460,650
EBITDA Q1	€ 14,560

TRINEXIA Africa

TRINEXIA Africa, formerly known as Cyber Security Africa Distribution (CSAD), has started positively for Q1, 2023 with a closing of € 1,839k of revenue for the period. The subsidiary unit has acquired these sales through 50% of new business, in addition to a growing professional services capability.

TRINEXIA Africa has begun the year with its face-to-face engagements with key partners and vendors for the entity. The deep collaboration with these stakeholders has underpinned its recent success, working closely to ensure the right solutions can be delivered. Further research and assessment have been undertaken on its planned territory expansion, with the necessary vendor and staff analysis to create the greatest return on new operational planning.

Notable deals from the quarter included a leading energy company in central Africa, and several large banking institutions, with a mixture of new and renewal business secured for TRINEXIA Africa within the continent.



Customers

CYBER1's customers range from government departments, large-scale industrial organisations, financial institutions, companies operating across the TMT sectors, national global communications carriers as well as SME sector businesses. Long-term exclusive relationships are the norm, especially when it comes to the technology that they are using.

Potential new clients are eager to learn about the services and successes that the Group have achieved and continue to implement. A few partnerships are being established with Government entities, globally.

Technology Partners

The Group continues to expand its partner network and now include but not limited to the following technologies: Anomali, Checkmarx, Checkpoint, Cribl, CyberArk, Cye, Dark Trace, Entrust, Exterro, Intel471, KnowBe4, Microsoft, Mimecast, Next DLP, Opentext, Palo Alto, Picus, Pulse Secure, Radware, Rapid7, Salt, Thales, Trellix, Trustwave and Zerofox.

Cash Flow

The revenue growth together with improved margin is starting to relieve some of the past year's operational cash flow pressure. The business continues to be subjected to competitive market conditions, macro environmental pressures, rising costs and inflation which does place stress on the Groups' free cash flow.

Improving cash flow is a key priority for the business and the Board together with the management team are looking at streamlining cash flow efficiencies through optimised accounts receivable processes and expense reduction strategies which will help improve financial stability and grow operations.

As the business continues to maintain a profit, it is important to note that generating cash from profits can take time, as profits need to be reinvested and managed effectively to ensure that they translate into positive cash flow.

FINANCIAL INFORMATION

Interim Report—Comparative Figures

The Q1 2023 report has not been formally reviewed by the Group's auditor.

Profit for the period

Group

Q1 2023 revenues amounted to €13,370k (Q1 2022: €9,487)

EBITDA for Q1 2023 amounted to €392k (Q1 2022: €-564k)

Profit before tax for Q1 2023 amounted to €206k (Q1 2022: €-689k)

Depreciation and amortisation for Q1 2023 amounted to €103k (Q1 2022: €127k)

There was a Net Cash inflow for Q1 2023, which amounted to €42k (Q1 2022: Net Cash outflow: €347k)

At the end of Q1 2023, the Group's cash balance amounted to €789k (Q1 2022: €525k)

Parent

The Parent Company's profit for Q1 2023 amounted to €31k (Q1 2022: profit of €24k)

Financial Position

Group

The Group's equity for end of Q1 2023 amounted to €4,475k (Q1 2022: €7,107k)

CYBER1 did not pay any dividends to shareholders during Q1 2023, 2022 and prior to this period.

Parent

The equity for the parent company amounted to €7,541k at the end of Q1 2023 (Q1 2022, €4,421k) and €6k in cash or cash equivalent for Q1 2023 (Q1 2022: €63k).

Share Information

Cyber Security 1 AB (Publ) (Trading as CYBER1) is a public company whose shares are traded on Nasdaq First North Growth Market (CYB1.ST)

The Company's share register is maintained by Euroclear Sweden AB.

Total number of registered shares by 31 March 2023 were: 1,025,928,865.

2023 Financial Calendar

First Quarter Report 2023	:	23 May 2022
Publication of 2022 Annual Report	:	5 May 2023
AGM 2023	:	26 May 2023
Half Year Report 2023	:	10 August 2023
Nine Month Report 2023	:	15 November 2023
Fourth Quarter Report 2023	:	28 February 2024

Accounting Principles

The interim report has been issued in accordance with International Financial Reporting Standards requirements (“IFRS”).

Risk and Uncertainties

Inherent risks and uncertainties for CYBER1 consist primarily of:

- Business risks concerning the delivery of contracted projects and payment.
- Financial risks (such as risks related to currency, interest rates, counterparties, future capital), market risks (e.g., competition, changes in demand) and risks related to the local conditions in the countries in which the Group conducts its business infrastructure.
- There are also risks of delays due to various disturbances in the delivery of contracted projects. Liquidity risk is managed through liquidity forecasting, which ensures sufficient funds are in place to meet the Group’s obligations and the overall strategy for the Group.

Certified Advisors

Mangold Fondkommission AB is appointed as the Certified Advisor for CYBER1.
Address:
Postal Address
Cyber Security 1 AB (CYBER1)
Box 70396
107 24 STOCKHOLM
CA@mangold.se
+46 8-503 015 50

Investor Relations

Please contact:
investor@cyber1.com

Auditors

The 2022 AGM resolved to elect RSM Stockholm AB, with Malin Lanneborn as auditor-in-charge, for the time up until the next annual general meeting in the company.

Election Committee and Extraordinary Annual General Meeting 2022

The Annual General Meeting in Cyber Security 1 AB (publ), reg. no 556135–4811, was held on 25 May 2022, by way of postal voting procedure.

The AGM resolved to re-elect Johan Bolsenbroek (Chairman), Alan Goslar, Pekka Honkanen, Zeth Nyström and Robert Brown (Executive Director), as Board Members.

Other resolutions considered and passed

Remuneration to the board of directors and auditors
It was resolved on a fee of SEK 450,000 to the chairman of the board and a fee of SEK 400,000 to each of the other board members, and that the auditor shall be remunerated in accordance with current approved accounts.

Resolution on incentive program 2022 for the board of directors and issue and transfer of warrants
It was resolved to adopt an incentive program 2022 for the board of directors and issue and transfer of warrants in accordance with a proposal submitted by a shareholder, whereby upon full exercise 11,250,000 new shares may be issued in the company.
The incentive program in summary can be found below. Shareholder's complete proposals for resolutions can be found at https://cyber1.com/corporate-governance/ (Comprehensive proposal LTI 2022 Board (Swedish) / Comprehensive proposal LTI 2022 Board (English)).

- Each stock option entitles the participant to acquire one (1) share in the company.
- The stock options will be granted without consideration to current and future board members.
- The program has a vesting period of 3 years (save for standard good leaver exceptions).
- For the stock options to vest, the company's (i) consolidated adjusted EBITDA per share and (ii) consolidated adjusted net revenue must, during a measurement period of in total twelve (12) calendar.

quarters, divided into three (3) sub-periods of four (4) calendar quarters each, have increased by an average of a certain minimum percentage point where the change is measured as the relative change in consolidated adjusted EBITDA per share and consolidated adjusted net revenue compared to the consolidated adjusted EBITDA per share and the consolidated adjusted net revenue during the four (4) calendar quarters immediately preceding the sub-period in question.

- Each stock option entitles the holder to acquire one (1) share in the company at an exercise price corresponding to 150 per cent of the volume-weighted average price for the company's share on Nasdaq First North during the period from and including 11 May 2022 up to and including 25 May 2022.

It was furthermore resolved to issue 11,250,000 warrants to the company to ensure the delivery of shares upon exercise of stock options under the incentive program.

Resolution on incentive program 2022 for employees and issue and transfer of warrants

It was resolved to adopt an incentive program 2022 for employees and issue and transfer of warrants in accordance with a proposal submitted by the board of directors, whereby upon full exercise 88,750,000 new shares may be issued in the company.
The incentive program in summary can be found below. The board's complete proposals for resolutions can be found at https://cyber1.com/corporate-governance/ (Comprehensive proposal LTI 2022 Staff (Swedish) / Comprehensive proposal LTI 2022 Staff (English)).

- Each employee stock option entitles the participant to acquire one (1) share in the company.
- The employee stock options will be granted without consideration to current and future employees of the company group.
- The program has a vesting period of three (3) years (save for standard good leaver exceptions) whereby a third of all stock options granted vests at each anniversary from grant.
- In order for the stock options to vest, the company's consolidated adjusted EBITDA per share must, during a measurement period of in total twelve (12) calendar quarters, divided into three (3) sub-periods of four (4) calendar quarters each, have increased by an average of certain minimum percentage point where the change is measured as the relative change in consolidated adjusted EBITDA per share compared to the consolidated adjusted EBITDA during the four (4) calendar quarters immediately preceding the sub-period in question.
- Each stock option entitles the holder to acquire one (1) share in the company at an exercise price corresponding to a per cent as set out below of the volume-weighted average price for the company's share on Nasdaq First North during the period from and including 11 May 2022 up to and including 25 May 2022 ("VWAP") as set out below.
    - First Sub-Vesting Period: 100 per cent of VWAP.
    - Second Sub-Vesting Period: 125 per cent of VWAP.
    - Third Sub-Vesting Period: 150 per cent of VWAP.

It was furthermore resolved to issue 88,750,000 warrants to the company to ensure the delivery of shares upon exercise of stock options under the incentive program.

Certification of Signatories

The Board of Directors certifies that the summarised interim report gives a true and fair view of the financial information in this report.

The Board of Cyber Security 1 AB (Publ), corporate identity number 556135-4811

Johan Bolsenbroek, Chairman, Non-executive Board member
Alan Goslar, Non-executive Board member
Pekka Honkanen, Non-executive Board member
Zeth Nyström, Non-executive Board member
Robert Brown, President, Executive Board member

DETAILED FINANCIAL INFORMATION

BALANCE SHEET	GROUP 31 March 2023	GROUP 31 March 2022	GROUP 31 December 2022	PARENT 31 March 2023	PARENT 31 March 2022	PARENT 31 December 2022
	€'000	€'000	€'000	€'000	€'000	€'000
ASSETS						
Non-current assets						
Property, plant and equipment	261	335	333	0	0	0
Right of use Asset	228	224	281	0	0	0
Intangible Assets	22	22	22	22	22	22
Investments in subsidiaries	0	0	0	4 942	2 321	4 942
Investments in associates	749	1 364	749	749	1 229	749
Other Non-Current Assets	0	0	0	0	0	0
Goodwill	6 728	6 630	6 735	0	0	0
Total Non-current assets	**7 987**	**8 575**	**8 120**	**5 713**	**3 572**	**5 713**
Current Assets						
Inventory	131	7	151	0	0	0
Deferred tax asset	140	125	145	0	0	0
Intercompany loans receivable	0	0	0	6 465	5 325	6 978
Trade and other receivables	28 406	18 959	23 500	1 147	444	410
Cash & Bank	789	525	747	6	63	111
Total Current Assets	**29 467**	**19 616**	**24 543**	**7 619**	**5 832**	**7 499**
TOTAL ASSETS	**37 454**	**28 191**	**32 663**	**13 331**	**9 404**	**13 212**
DEBT AND EQUITY CAPITAL						
Equity Capital						
Share Capital	269	186	267	269	186	267
Share premium	27 340	24 390	27 414	27 340	24 293	27 318
Retained Earnings	-22 746	-17 500	-23 078	-20 067	-20 059	-20 139
Other Reserves	0	0	0	0	0	0
Non Controlling Interest	-388	31	-453	0	0	0
Total Equity	**4 475**	**7 107**	**4 150**	**7 541**	**4 421**	**7 446**
Non-current liabilities						
Interest-bearing liabilities	5 028	0	5 028	5 028	0	5 028
Total Non-current liabilities	**5 028**	**0**	**5 028**	**5 028**	**0**	**5 028**
Current liabilities						
Interim Debt	3 951	3 951	3 951	0	0	0
Lease liabilities	305	392	366	0	0	0
Bank Overdraft	599	1 761	1 610	0	0	0
Intragroup Debt	0	0	0	342	445	275
Trade and other payables	19 124	12 573	16 070	418	4 577	474
Tax payable	373	357	216	2	-38	-11
Provisions	3 599	2 050	1 272	0	0	0
Total current liabilities	**27 951**	**21 084**	**23 485**	**762**	**4 983**	**738**
Total Liabilities	**32 979**	**21 084**	**28 513**	**5 790**	**4 983**	**5 766**
TOTAL DEBT AND EQUITY	**37 454**	**28 191**	**32 663**	**13 331**	**9 404**	**13 212**

	GROUP		
Statement of comprehensive income (loss)	**Jan - Mar 2023**	**Jan - Mar 2022**	**Jan - Dec 2022**
	€'000	€'000	€'000
Continuing operations			
Net Revenue	13 370	9 487	46 833
Cost of Sold Goods	-10 257	-7 596	-37 520
Gross Profit	**3 113**	**1 892**	**9 313**
Sales Costs	-2 063	-1 833	-8 460
Administration Costs	-658	-623	-3 950
Depreciation	-103	-127	-541
Total Operating Cost	**-2 824**	**-2 583**	**-12 951**
Operating Result	**289**	**-691**	**-3 638**
EBITDA	**392**	**-564**	**-3 097**
Financial income and costs			
Finance income	0	16	151
Finance costs	-58	-67	-310
Other financial items	-25	54	-54
Total Finance income and costs - net	**-83**	**3**	**-213**
Share of net profit of associates accounted for using the equity method	**0**	**0**	-15
Result before tax	**206**	**-689**	**-3 866**
Tax (Period)			
Net income for the period, continuing operations	**206**	**-689**	**-3 866**
Net income	**206**	**-689**	**-3 866**
Net income (loss) attributable to:			
Owners of the Parent Company	193	-534	-3 173
Non-controlling interests	13	-154	-693

	PARENT		
Statement of comprehensive income (loss)	**Jan - Mar 2023**	**Jan - Mar 2022**	**Jan - Dec 2022**
	€'000	€'000	€'000
Continuing operations			
Net Revenue	245	169	714
Cost of Sold Goods	0	0	0
Gross Profit	**245**	**169**	**714**
Sales Costs	-106	-18	-56
Administration Costs	-108	-129	-631
Depreciation	0	0	0
Total Operating Cost	**-214**	**-147**	**-687**
Operating Result	**32**	**22**	**27**
EBITDA	**32**	**22**	**27**
Financial income and costs			
Finance income	0	0	0
Finance costs	-0	0	-16
Other financial items	-0	1	-28
Total Finance income and costs - net	**-0**	**1**	**-44**
Share of net profit of associates accounted for using the equity method	0	**0**	0
Result before tax	**31**	**24**	**-17**
Tax (Period)	0	0	**0**
Net income for the period	**31**	**24**	**-17**

CASH FLOW ANALYSIS	Group		
	Jan - Mar 2023	Jan - Mar 2022	Jan-Dec 2022
	€ '000	**€ '000**	**€ '000**
Profit before income taxes	206	-689	-3 866
Retained Earnings Adjustments	-80	0	0
Other Non-Cash Items	-4	0	10
Movements in Provisions	2 136	0	0
Depreciation	103	135	541
Interest Paid	-51	-40	-310
Interest Received	0		151
Changes in Working Capital	**-1 710**	**-955**	**-1 117**
Cash Flow from Operations	**601**	**136**	**-4 591**
Paid Taxes	90	66	-233
Cash Flow from Operating Activities	**691**	**202**	**-4 824**
Acquisition of subsidiaries	0	0	0
Investment in Associates	0	-135	-276
Acquisition of Fixed Assets	-5	-114	-514
Cash Flow from Investment Activities	**-5**	**-249**	**-790**
New share issues	60	0	3 105
Proceeds from ongoing share issue	0	0	0
Lease liabilities	-50	-48	-65
Borrowings	-631	-252	5 028
Cash Flow from Financing Activities	**-621**	**-300**	**8 068**
Change in cash and cash equivalents during the year			
Net change in cash, continuing operations	65	-347	2 454
Net change in cash, discontinued operations	0	0	0
Foreign exchange translation reserves	-23	0	-2 579
Opening Cash position	747	872	872
Closing Cash Position	**789**	**525**	**747**

CONSOLIDATED STATEMENT OF CHANGES IN EQUITY	Jan - Mar 2023	Jan - Mar 2022	Jan-Dec 2022
	€ '000	€ '000	€ '000
Equity - Opening Balance	**4 150**	**7 803**	**7 803**
Adjustment from acquisition analysis			0
Share Issues	0	0	3 105
Profit from the Period	206	-689	-3 866
Foreign Exchange-Differential	**119**	-7	-2 893
Changes in equity during the period	**325**	**-696**	**-3 654**
Equity - Closing Balance	**4 475**	**7 107**	**4 150**

PARENT STATEMENT OF CHANGES IN EQUITY	Jan - Mar 2023	Jan - Mar 2022	Jan-Dec 2022
	€ '000	€ '000	€ '000
Equity - Opening Balance	**7 446**	**4 403**	**4 403**
Adjustment from acquisition analysis		0	0
Share Issues	0	0	3 105
Profit from the Period	31	24	-17
Foreign Exchange-Differential	64	-6	-45
Changes in equity during the period	**95**	**18**	**3 043**
Equity - Closing Balance	**7 541**	**4 421**	**7 446**

NOTES TO THE INTERIM FINANCIAL STATEMENTS

Note 1 – General accounting principles

CYBER1 (the Group) consists of Cyber Security 1 AB (the Company) and its subsidiaries. Cyber Security 1 AB is a public company, incorporated in Sweden. The consolidated interim financial statements consist of the Group and the Parent company and Group's subsidiary companies. As a result of rounding differences, numbers or percentages may not add up to the total. These interim condensed consolidated financial statements for the nine months ending 31 December 2022, have been prepared in accordance with IAS 34 Interim Financial Reporting as issued by the International Accounting Standards Board (IASB) and the Swedish Annual Accounts Act, and for the parent company in accordance with the Swedish Annual Accounts Act and RFR 2 Reporting for legal entities and other statements issued by the Swedish Financial Reporting Board. The interim condensed consolidated financial statements do not include all the information and disclosures required in the annual financial statements and should be read in conjunction with the Group's annual financial statements for 2020 (Annual Report 2020). Key developments in risks and uncertainties, including COVID-19, are described in the section Risks and uncertainties.

IASB has published amendments of standards that are effective as of 1 January 2020 or later. The standards have not had any material impact on the financial reports.

On 28 May 2020, IASB issued Covid-19-Related Rent Concessions, which amended IFRS 16 Leases. The amendment permits lessees, as a practical expedient, not to assess whether particular rent concessions occurring as a direct consequence of the Covid-19 pandemic are lease modifications and instead to account for those rent concessions as if they are not lease modifications. The amendment does not affect lessors. On 12 October 2020, the European Union has published a Commission Regulation endorsing of the Amendment to IFRS 16 Leases Covid-19-Related Rent Concessions. The Amendments are effective for annual periods beginning on or after 1 June 2020.

IBOR transition

Where interest rate hedge accounting is applied CYBER1 is exposed to the STIBOR (Stockholm Interbank Offered Rate) reference rate for hedged instruments together with their hedging instruments. The change of reference rate due to the upcoming IBOR transition will, when implemented, affect future cash flows on interest income and interest expense but CYBER1 expects continued 100% effectiveness of the hedges and no net interest impact. CYBER1 will continue to monitor any changes to STIBOR as a reference rate and update, together with counterparties, the relevant financial contracts accordingly as and when these occur.

Items affecting comparability

CYBER1 reports an adjusted EBIT for comparison reasons. The result is adjusted for capital gains and losses from divestments and larger restructuring initiatives and impairments.

Loss of control of a wholly owned subsidiary with an interest retained.

When the group disposes of a significant part of its interest, and therefore loses control, of a subsidiary, the group de-consolidates the subsidiary. If the retained interest in the entity fulfils the criteria of being an associate, it is accounted for at fair value at the disposal date, and subsequently accounted for using the equity method. The gain or loss of the transaction is the difference between the fair value of the consideration received as well as the fair value of the retained interest, and the carrying value of the former subsidiary's net assets (including any related goodwill) and is recorded in the income statement. Any portion of the gain or loss related to the re-measurement of the retained interest to fair value is disclosed separately.

Impact on the financial reporting due to COVID-19

Goodwill

During the reporting period to March 2023, CYBER1 has outlined the cash-generating units (CGUs) within the business area of CYBER1 Group. The recoverable amount of all of the CGUs has been assessed based on estimates of value in use. Calculations of value in use are based on the estimated future cash flows using forecasts covering a five-year period, which are in turn based on the three-year plans prepared annually by each of the business areas and approved by CYBER1 Group Executive Management.

These plans are founded on the business areas' strategies and an analysis of the current and anticipated business climate, and the impact this is expected to have on the market in which the business area operates. A range of economic indicators, which differ for each market, and external and internal studies of these, are used in the analysis of the business situation. The forecasts form the basis for how the values of the material assumptions are established.

The assumptions mentioned below reflect past experience and are consistent with external information. The most material assumptions when determining the value in use include anticipated demand, growth rate, operating margin, working capital requirements and the discount rate.

The factor used to calculate growth in the terminal period after five years was 2% (in line with last year). Need of working capital beyond the five-year period is deemed to increase approximately as the expected growth in the terminal period. The discount rate consists of a weighted average cost of capital for borrowed capital and shareholders' equity. Since 2020 CYBER 1 calculates a pre-tax discount rate for each CGU. As of March, it varied between 9.3% and 13.5%. Last year all CGUs applied a pre-tax discount rate of 11% before tax. The specific risks of the CGUs have been adjusted in the future cash flow forecasts.

Impairment tests were performed in response to the Covid-19 pandemic. The testing of goodwill did not indicate any impairment requirement. Sensitivity in the calculations implies that the goodwill value would be maintained even if the discount rate was increased by 2 percentage points or if the long-term growth rate was lowered by 2 percentage points. The goodwill value would also be maintained, given an operating margin drop by 2 percentage points.

Inventory

As of 31 March 2023, there is no significant impact on the valuation of inventory related to the Covid-19 pandemic.

Expected credit losses

As of 31 March 2023, there are no indications on any significant impact related to the Covid-19 pandemic. Expected credit losses remain on a low level compared to twelve months rolling revenues.

Note 2 – Operating segment information

Revenue and Segments

CYBER1 is located in three main regions, namely: Africa, Europe, and the Middle East, with more than 160 employees.

For management and reporting purposes, the Group is organised by these geographical areas.

The performance of these geographical areas is evaluated on a regular basis by CYBER1's executive team, consisting of among others, the Managing Directors of each geographical segment. In addition to the geographical areas, the Group operates Shared Services functions and central administration. These costs are reported separately as Group Shared Services and Group costs.

Revenue per Segment	Jan - Mar 2023	Jan - Mar 2022
	€ '000	€ '000
Africa	10 383	6 308
Middle East	3 340	3 316
Europe	68	15
Sub-Total including internal Sales	**13 791**	**9 639**
Internal Sales and Eliminations	-422	-151
Segment Total	**13 370**	**9 487**

For management and reporting purposes, Cyber Security 1 AB is included in Group Shared Services. The corresponding information from earlier periods is restated. Transfer prices between operating segments are on arm's length basis in a manner similar to transactions with third parties.

Disaggregation of revenue in the following table, revenue is disaggregated by major revenue streams divided into the reportable segments as shown below:

Georgraphical information - Current Year	Revenue	Adjusted organic growth	EBITDA	EBITDA margin	Non-current assets
	€ '000	%	€ '000	%	€ '000
Jan - Mar 2023					
Africa	10 383	65%	240	2%	411
Middle East	3 340	1%	85	3%	176
Europe	68	367%	-3	-4%	5 713
Core business	**13 791**	**43%**	**322**	**2%**	**6 300**
Internal Sales and Eliminations	-422	178%	70	-17%	1 688
Cyber1 Group	**13 370**	**41%**	**392**	**3%**	**7 987**

Georgraphical information - Prior Year	Revenue	Adjusted organic growth	EBITDA	EBITDA margin	Non-current assets
	€ '000	%	€ '000	%	€ '000
Jan - Mar 2022					
Africa	6 308	2%	-449	-71%	519
Middle East	3 316	-41%	27	8%	38
Europe	15	-97%	-16	-1067%	8 038
Core business	**9 639**	**-50%**	**-437**	**-45%**	**8 595**
Internal Sales and Eliminations	-151	-1%	-127	837%	-20
Cyber1 Group	**9 487**	**-51%**	**-564**	**-59%**	**8 575**

Georgraphical information - Current Year	Distribution	Solutions	Next Gen SOC	Jan - Mar 2023
	€ '000	€ '000	€ '000	€ '000
Jan - Mar 2023				
Africa	3 342	6 932	108	10 383
Middle East	2 808	532	0	3 340
Europe	68	0	0	68
Including internal sales	**6 219**	**7 464**	**108**	**13 791**
Internal Sales and Eliminations				-422
Total				**13 370**

Georgraphical - Prior year	Distribution	Solutions	Next Gen SOC	Jan - Mar 2022
	€ '000	€ '000	€ '000	€ '000
Jan - Mar 2022				
Africa	251	6 058	0	6 308
Middle East	3 313	3	0	3 316
Europe	15	0	0	15
Including internal sales	**3 578**	**6 060**	**0**	**9 639**
Internal Sales and Eliminations		0	0	-151
Total				**9 487**

Note 3 - Financial instruments

CYBER1 is exposed to a number of financial market risks that the Group is responsible for managing under the finance policy approved by the Board of Directors. The overall objective is to have cost-effective funding in the Group companies. The financial risks in the Group are managed, to a limited extent, through the use of financial instruments. The main exposures for the Group are liquidity risk, interest rate risk and currency risk.

Derivatives for currency hedging are measured at fair value, according to level 2, in compliance with IFRS 13. Other financial instruments are measured at their carrying amounts.

The significant financial assets and liabilities are shown below. According to CYBER1's assessment, there is no significant difference between the carrying amounts and fair values

CYBER1's financial assets consist mainly of receivables from end customers, other operators and resellers as well as cash and cash equivalents. CYBER1's financial liabilities consist mainly of loans, lease liabilities and accounts payables. For the category "Liabilities to financial institutions and similar liabilities" the reported value amounted, at 31 December 2022, to €849k (2021 : €1,500k).

Carrying value and fair value

CYBER1 applies IFRS 9 to classify and measure financial instruments.

Cyber Security 1 AB uses the following valuation techniques of the fair value hierarchy in determining the fair values of the financial instruments:

Level 1 - Quoted prices (unadjusted) in active markets
Level 2 - Inputs other than quoted prices that are observable, either directly or indirectly
Level 3 - Inputs that are not based on observable market data

The accounting principles related to financial liabilities are essentially unchanged compared with previous years. CYBER1 has updated its accounting principles related to expected credit losses and has, in accordance with the standard, implemented the "expected loss model."

Disclosures on financial instruments

The following table shows the carrying amounts and fair values for the individual classes of financial instruments as well as the fair value hierarchy for the assets and liabilities that are measured at fair value in the balance sheet.

Carrying value and fair value — as at March 2023

	Financial instruments measured at FVTPL	Financial assets measured at amortized cost	Other financial liabilities	Cash flow hedges measured at FVOCI	Other receivables and liabilities	Total carrying value	Estimated fair value
	€'000	€'000	€'000	€'000	€'000	€'000	€'000
Trade receivables		26 817			1 589	28 406	28 406
Other non-current financial receivables						0	0
Other current assets and financial receivables					270	270	270
Prepaid expenses and accrued income						0	0
Cash and cash equivalents		789				789	789
Total assets	**0**	**27 607**	**0**	**0**	**1 859**	**29 466**	**29 466**
Loans and borrowings			3 951			3 951	3 991
Other non-current financial liabilities					0	0	0
Other current liabilities			1 276			1 276	1 276
Accrued expenses and deferred income					3 599	3 599	3 599
Trade payables			19 124			19 124	19 124
Total liabilities	**0**	**0**	**24 351**	**0**	**3 599**	**27 951**	**27 990**

Fair value measurement by level

	Level 1	Level 2	Level 3	Total
	€'000	€'000	€'000	€'000
Derivative financial assets	-	-	-	-
Derivative financial liabilities	-	-	-	-

Carrying value and fair value — as at March 2022

	Financial instruments measured at FVTPL	Financial assets measured at amortized cost	Other financial liabilities	Cash flow hedges measured at FVOCI	Other receivables and liabilities	Total carrying value	Estimated fair value
	€'000	€'000	€'000	€'000	€'000	€'000	€'000
Trade receivables		18 959				18 959	18 959
Other non-current financial receivables						0	0
Other current assets and financial receivables					132	132	132
Prepaid expenses and accrued income					0	0	0
Cash and cash equivalents		525				525	525
Total assets	**0**	**19 484**	**0**	**0**	**132**	**19 616**	**19 616**
Loans and borrowings			3 951			3 951	3 951
Other non-current financial liabilities						0	0
Other current liabilities			2 510			2 510	2 510
Accrued expenses and deferred income					2 050	2 050	2 050
Trade payables			12 573			12 573	12 573
Total liabilities	**0**	**0**	**19 034**	**0**	**2 050**	**21 084**	**21 084**

Fair value measurement by level

	Level 1	Level 2	Level 3	Total
	€'000	€'000	€'000	€'000
Derivative financial assets	-	-	-	-
Derivative financial liabilities	-	-	-	-

Financial instruments, level 2

The fair value of financial instruments that are not traded on an active market are determined by means of available valuation techniques. Market information is used when available. The use of corporate-specific information is avoided whenever possible. If all important in-data required for a fair value valuation of an instrument is observable, the instrument is in level 2. Specific valuation techniques used in the valuation of financial instruments include, for example, listed market prices, fair value for interest-rate swaps, calculated as the present value of estimated future cash flows based on observable yield, fair value of currency forward contracts determined through the use of rates for currency foreign exchange contracts on the balance sheet date.

DISTRIBUTION BY LEVEL WHEN MEASURED AT FAIR VALUE	31 March 2023				31 March 2022			
	Level 1	Level 2	Level 3	Total	Level 1	Level 2	Level 3	Total
	€'000	€'000	€'000	€'000	€'000	€'000	€'000	€'000
FINANCIAL ASSETS								
Financial assets measured at fair value through profit or loss:								
Derivative financial instruments – non-hedge accounting								
Derivatives used for hedging purposes:								
Derivative financial instruments – hedge accounting								
Total financial assets	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
FINANCIAL LIABILITIES								
Financial liabilities at fair value through profit or loss:								
Derivative financial instruments – non-hedge accounting								
Contingent considerations			40	40			45	45
Derivatives used for hedging purposes:								
Derivative financial instruments – hedge accounting								
Total financial liabilities	**0**	**0**	**40**	**40**	**0**	**0**	**45**	**45**

Financial instruments, level 3

The change during the quarter for instruments at level 3 refers to contingent considerations. Contingent considerations are valued at the fair value based on data available such as conditions set forth in the purchase agreement and current assessments of the estimated fulfilment of the conditions.

MOVEMENTS FINANCIAL INSTRUMENTS LEVEL 3			
Contingent considerations	**Q1 2023**	**Q1 2022**	**Full year 2022**
	€'000	€'000	€'000
Opening balance	0	0	0
Business combinations			
Payments	0	0	0
Reversals			
Revaluations	40	0	0
Translation differences			
Closing balance	**40**	**0**	**0**

No transfer in or out of level 3 or level 2 has been made during the quarter to March. The recognised amounts are regarded as reasonable estimates for all items measured at carrying value in the balance sheet, except for loans and borrowings, as these amounts have a long time to maturity.

The fair value of loans and borrowings differ from their carrying value as a consequence of changes in the market interest rates. Items not valued at fair value in the balance sheet are measured at amortised cost.

Note 4 – Significant Events

There were no significant events during the quarter under review.

Note 5 – Impairments

Goodwill and Disposal of non-current assets

An impairment test on goodwill in accordance with IAS 36 (Impairment of Assets) is generally performed annually within the Cyber Security 1 AB Group, in the fourth quarter once the operational three-year plan has been prepared or if there are indications for impairment. In this impairment test, the carrying amount of a group of cash-generating units (CGUs) to which goodwill is allocated is compared with the recoverable amount of this group of CGUs.

No impairments have been deemed necessary in the current reporting period.

Note 6 – earnings per share

Earnings per share	Jan - Mar 2023	Jan - Mar 2022
	€ '000	€ '000
Profit for the period	**206**	-689
Non-controlling interests	**13**	-154
Group share of profit	**193**	-534
Number of shares (weighted average)	**1 023 621**	866 058
Earnings per share	**0.0019**	-0.0062
Net income from continuing operations – attributable to the parent entity	**193**	-534

There has been no material change to the contractual obligations during the current reporting period.

Note 8 - Significant risks and uncertainties

As a decentralised company with operations across the Global, CYBER1 faces internal and external risks that may impact its ability to achieve strategic objectives and financial targets. The Group is active in the design, implements and manages solutions that protect critical IT infrastructure, data assets, independent product advice and professional services across all cybersecurity application spaces.

The general identified risks are mainly within the following categories: financial, operational, contract and assignment, IT, sustainability, governance and branding. CYBER1 has a risk management process in place which is part of the CYBER1 Model. Successful risk mitigation creates opportunities and competitive advantages.

CYBER1 Group operates in a broad range of geographical product and service markets in the highly competitive and regulated cyber security industry. CYBER1 has defined risk as anything that could have a material adverse effect on the achievement of CYBER1 Group's goals. Risks can be threats, uncertainties or lost opportunities relating to CYBER1's current or future operations or activities.

CYBER1 has an established risk management framework in place to regularly identify, analyse, assess and report business, financial as well as ethics and sustainability risks and uncertainties, and to mitigate such risks when appropriate. CYBER1 Group's risk universe consists of four categories and over thirty risk areas used to aggregate and categorise risks identified across the business within the risk management framework, see below.

For further information regarding details on risk exposure and risk management, see the Annual Report 2022, Directors Report and the newly published Governance report.

Note 9 - Related parties Related party transactions

There have been no significant changes in the relationships or transactions with related parties for the Group or Parent Company with the information given in the annual report 2022.

Other- Parent Company

The consolidated figures in this report are presented at the consolidated level for Cyber1 AB. The Parent Company, Cyber Security 1 AB (corporate identity number 556135-4811), directly and indirectly holds 100% of the shares in all subsidiaries in the Group, except for the companies in South Africa, in which the non-controlling interest is 26% in CYBER1 Solutions Southern Africa and TRINEXIA Southern Africa.

Sweden

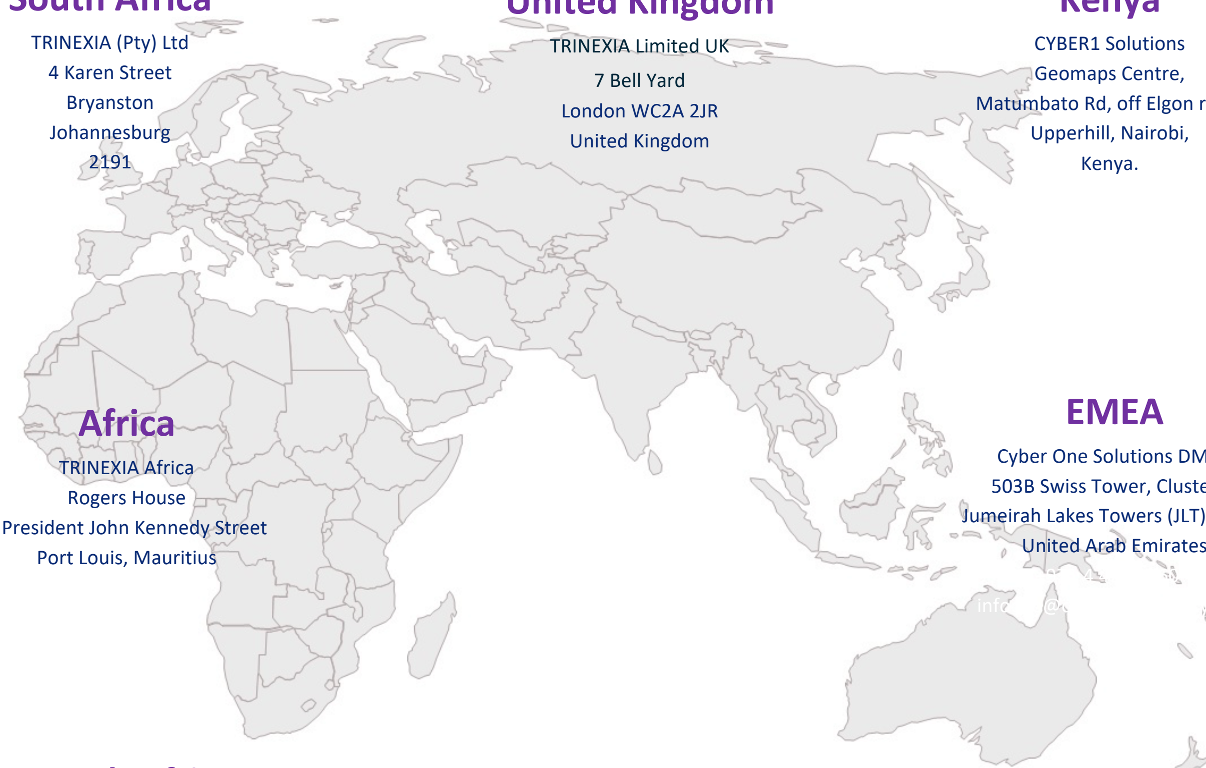
Cyber Security 1 AB (Cyber1)
Klarabergsviadukten 70, D4 , 111
64 Stockholm
Box 70396
107 24 Stockholm

Middle East & India

TRINEXIA DMCC
504 Swiss Tower, Cluster Y,
Jumeirah Lakes Towers (JLT), Dubai
United Arab Emirates

South Africa

CYBER1 Solutions (Pty) Ltd
46A Wierda Rd West
Wierda Valley
Johannesburg
2146



South Africa

TRINEXIA (Pty) Ltd
4 Karen Street
Bryanston
Johannesburg
2191

United Kingdom

TRINEXIA Limited UK
7 Bell Yard
London WC2A 2JR
United Kingdom

Kenya

CYBER1 Solutions
Geomaps Centre,
Matumbato Rd, off Elgon road,
Upperhill, Nairobi,
Kenya.

Africa

TRINEXIA Africa
Rogers House
5 President John Kennedy Street
Port Louis, Mauritius

EMEA

Cyber One Solutions DMCC
503B Swiss Tower, Cluster Y,
Jumeirah Lakes Towers (JLT), Dubai
United Arab Emirates

South Africa

Credence Security (Pty Ltd
Karen Street
Bryanston 2021
South Africa

South Africa

Cyber1 SOC (Pty) Ltd
Block H
Peter Place Office Park
54 Peter Place Road
Bryanston

Johannesburg

2191