11 April 2019

Corero Network Security plc

("Corero", "Company" or the "Group")

Full year results

Corero Network Security plc (AIM:CNS), the AIM listed network security company, announces its audited results for the year ended 31 December 2018.

Financial Highlights:

- Group revenue of $10.0 million (2017: $8.5 million) of which 51.1% is recurring
  - SmartWall revenue up 23.1%
  - SmartWall recurring revenue[1] up 43.2%
- Significantly reduced EBITDA[2] loss of $2.1 million (2017: loss $5.0 million[3])
- Adjusted operating costs[4] 13.3% below 2017
- Loss before tax of $5.2 million (2017: loss $8.5 million[3])
- Loss per share 1.4 cents (2017: loss per share 3.0 cents[3])
- Successful equity fund raise in April 2018 of $5.3 million (after costs)
- $2.0 million investment from Juniper Networks (NYSE: JNPR) secured in October 2018
- Strong balance sheet with net cash at 31 December 2018 of $4.4 million (2017: $1.4 million)

Operating Highlights:

- Signed global resale partnership with Juniper Networks (NYSE: JNPR)
- Increase in average new customer order intake value:
  - Perpetual license sales orders $275,000 (2017: $250,000)
  - As-a-service contract value $55,000 per annum (2017: $40,000)
- Follow-on orders from existing customers up 57% to $4.4 million (2017: $2.8 million)
- Continued high levels of customer satisfaction
  - Services renewal rate remained strong at 98.5% (2017: 97.5%)

Outlook

- Entered 2019 with a growing new business pipeline from both new and existing customers
- New Juniper resale partnership now set to deliver incremental revenue growth, with first revenue generating order secured in March 2019
- DDoS mitigation market fundamentals remain strong with market analysts forecasting double digit growth
- The Board continues to believe the business is well-placed for further growth

Ashley Stephenson, CEO of Corero, commented:

"2018 was a year of continued strategic progress for Corero, culminating in the signing of a landmark resale partnership with Juniper Networks, a US-based industry leader in automated, scalable and secure networks. Not only does this agreement provide an additional route to market for our products but it also serves as a significant endorsement of our SmartWall technology. Securing the first Juniper resale customer win in March 2019 was a significant milestone in the development of the Juniper go-to-market channel for Corero.

"Corero continues to be well positioned to deliver on its goal of becoming the leading player in the real-time DDoS mitigation market, with over 100 customers and a growing number of go-to-market partners.

"We remain focused on delivering strong revenue growth and committed to achieving our stated goal of being EBITDA positive and cash generative by the end of the year."

Enquiries:

Corero Network Security plc
Andrew Miller, CFO Tel: 01895 876 382

Cenkos Securities plc Tel: 020 7397 8900
Mark Connelly – NOMAD
Michael Johnson – Sales

Vigo Communications Tel: 020 7390 0230
Jeremy Garcia / Antonia Pollock / Charlie Neish
corero@vigocomms.com

About Corero Network Security

Corero Network Security is a leader in real-time, high-performance DDoS defense solutions. Service providers, hosting providers and digital enterprises rely on Corero's award winning technology to eliminate the DDoS threat to their environment through automatic attack detection and mitigation, coupled with complete network visibility, analytics and reporting. This industry leading technology provides cost effective, scalable protection capabilities against DDoS attacks in the most complex environments while enabling a more cost effective economic model than previously available. For more information, visit www.corero.com

Operational review

2018 represents another period of strategic progress for Corero. Revenue for the year was $10.0 million (2017: $8.5 million), comprising almost entirely of sales from SmartWall, Corero's market leading DDoS mitigation solution, which grew by 23.1% in 2018. Recurring revenue, comprising security maintenance and support services and DDoS protection as-a-service revenue, increased to 51.1% of total revenue versus 47.1% in the prior year.

Corero closely managed costs in 2018, with adjusted operating expenses[4] of $9.9 million, 13.3% below the prior year (2017: $11.4 million[3]). In addition, the EBITDA[2] loss for the year reduced to $2.1 million (2017: loss $5.0 million[3]).

Revenue growth and progress towards EBITDA break-even was impacted by the longer than anticipated time required to secure contracts and develop revenues from new go-to-market partners in the year. However, we expect this to ramp-up in 2019.

The loss for the year reflects the continuing investment in Corero's technology and sales and marketing activities. Management is focused on delivering revenue growth, adding new customers, and targeting being EBITDA positive and cash generative by the end of 2019, by focusing on:

- Executing on a strong and growing pipeline including opportunities arising from the recently announced Juniper resale partnership; and
- Leveraging the growing demand for Corero 100Gbps SmartWall technology from the adoption of faster and more economic 100Gbps links in the Company's target markets.

Corero continued to make good operational progress during 2018, delivering against the 2018 strategic objectives which included:

Expanding routes to market: Signed global resale partnership with Juniper Networks in September 2018; partnership enabled with product SKUs, sales and support training. Both Corero and Juniper are now actively engaged with a number of prospects and trials with a strong pipeline of Juniper customer resale opportunities developing.

Growing customer base: Progress made in the year, with new customer acquisition to be accelerated with ongoing demand for Corero's SmartWall solution (over 100 SmartWall customers at year end); over $1.5 million order intake for SmartWall 100Gbps product in 2018 (2017: $0.4 million from initial orders following product release in December 2017); Juniper global resale partnership is expected to increase customer numbers in 2019; sales order intake from Digital Enterprise customers grew by 53%.

Maintaining competitive advantage in real-time DDoS mitigation: Delivered two new major SmartWall software releases to customers; developed the SmartWall Threat Defense Director ("TDD") product, a market leading DDoS mitigation software solution for large Tbps scale networks, for the Juniper global resale partnership; released fully integrated 100Gbps DDoS Appliance – the SmartWall NTD1100, a market leading solution for migration to 100Gpbs connectivity.

Financial Summary

The Group reported revenues of $10.0 million (2017: $8.5 million).

Total operating expenses were $12.7 million (2017: $14.9 million[3]).

- Operating expenses net of capitalised R&D costs and before depreciation and amortisation of intangible assets were $9.4 million (2017: $12.0 million[3]). Capitalised R&D costs were $1.7 million (2017: $2.2 million).
- Operating expenses include an unrealised exchange gain of $0.4 million (2017: loss $0.6 million) arising from an intercompany loan.
- Depreciation and amortisation of intangible assets was $3.3 million (2017: $3.0 million).

Losses before taxation were $5.2 million (2017: loss $8.5 million[3]) including amortisation of capitalised R&D of $2.9 million (2017: $2.4 million). The reported loss per share fell to 1.4 cents (2017: loss per share 3.0 cents[3]).

Corero had net cash of $4.4 million at 31 December 2018 (2017: $1.4 million), comprising:

- Cash at bank of $8.0 million as at 31 December 2018 (2017: $1.4 million), having raised $5.3 million (after costs) in April 2018 from an equity placing and subscription, $3.9 million (net of costs) from a bank term loan concluded in April 2018 and drawn down in May 2018 (the "Debt Facility"), and $2.0 million from an equity subscription by Juniper Networks in October 2018; and
- Debt of $3.6 million (2017: nil) comprising the Debt Facility. The Debt Facility replaced an existing accounts receivable financing facility of $1.5 million.

The net cash used in operating activities in the year ended 31 December 2018 was $1.8 million (2017: net cash used $6.0 million) reflecting the loss for the year and increase in working capital investment in the period of $0.3 million (2017: increase in working capital investment $0.7 million).

Market Dynamics

Technology continues to promise significant enhancements to business models in terms of both driving competitiveness and revenue growth through the deployment of digital strategies and technology platforms. However, as reported in the World Economic Forum Global Risks Report for 2019, technology also continues to play a profound role in shaping the global risks landscape, with cyber attacks remaining one of the top 5 global risks in terms of likelihood.

Along with email spam, phishing, and malware, DDoS attacks remain a persistent blight on the Internet. Technically sophisticated attackers using automated methods for launching attacks have escalated an occasional but often severe nuisance into a widespread, ever-present and constantly worsening threat. Corero's Full Year 2018 DDoS Trends Report shows the average number of attacks per customer was up 16% over 2017.

Financially motivated criminal organisations and nation state actors bent on cyber warfare have combined forces with malicious hackers to pool knowledge and experience to launch increasingly complex, multi-vector attacks that are more difficult to detect and mitigate. The vast majority of DDoS attacks are still either volumetric in nature – consuming a high percentage of network bandwidth – or focused on exhausting protocol-processing resources in the host systems under attack. Both types are highly effective in knocking out Internet applications and services, for minutes to sometimes hours and with negative consequences for service providers, businesses and consumers.

Attacks are often launched utilising large-scale botnets that attackers create by hijacking poorly secured endpoints, including servers, PCs, laptops and, in recent years, consumer IoT devices such as webcams. The majority (according to Verizon, over 75%) still leverage amplification techniques that jack up attack intensity by exploiting vulnerabilities in Internet services and host systems to increase the flood of traffic directed at targets.

The vast complex of public networks spanning the globe is constantly growing and evolving, reaching into every corner of society. New users, endpoints and networks come online every hour of every day, presenting bad actors with a constantly expanding surface with new targets potentially vulnerable to attacks or exploitable for launching them.

Internet evolution is shifting the DDoS battlefield in two directions: out towards the rapidly growing IoT edge and up into the hyperscale datacentres supporting the ever-expanding cloud.

Rapid IoT adoption is driving a proliferation of intelligent devices that will ultimately exceed the number of user endpoints. Machine-to-machine connections from the edge will power a wide range of IoT applications, healthcare, environmental sensing and "smart" infrastructure – cities, buildings, homes and vehicles. Cybercriminals have already hijacked consumer IoT devices to create large-scale botnets and emerging mission-critical IoT networks will become targets for potentially catastrophic DDoS attacks.

Cloud-based services supporting mobile apps, streaming video, e-commerce, SaaS and enterprise IT are growing at an astounding rate, deployed in massive hyperscale data centres consisting of thousands of servers, which are both targets for attack and potential launch platforms. Content delivery networks that are instrumental in scaling cloud service delivery, are also targets for crippling attacks that can disrupt services for millions of users.

Bandwidth at the Internet edge continues to scale up. Gigabit consumer broadband is here, now. Multi-gigabit wireless over 5G networks is just over the horizon. More bandwidth at the edge is driving more capacity in the backbone. Service provider Internet connections are moving from 10Gbps to 100Gbps. A faster edge enables higher intensity attacks, and fewer endpoints are needed to launch crippling volumetric attacks.

DDoS defence is still a never-ending battle. Attackers discover and exploit vulnerable hosts or services to launch attacks. Defenders monitor network activity to compile a catalogue of attack profiles that are then used to generate rules to detect and identify attacks to take the necessary mitigation actions.

Opportunities for Corero

Adoption of faster 100Gbps links

As transit providers start pushing tenants towards using fractional committed data rates on 100Gbps connections for cost and efficiency, versus two or more individual 10Gbps connections, we expect increased adoption of 100Gbps links. The challenge with faster 100Gbps links is that tenants can then be hit by up to 100Gbps of attack traffic, even if they are only subscribing to 20Gbps of regular capacity.

We anticipate demand for Corero's SmartWall 100G technology to accelerate as a result of this and increasing end-user service-level expectations resulting in the requirement for Service Providers, Cloud Providers and Enterprises to deploy DDoS mitigation technology upgrades. Corero's 100Gbps line-rate appliance ensures each 100Gbps connection can be automatically protected from DDoS, without impacting legitimate traffic.

5G will increase DDoS attack risk

Telecoms providers are in a race to rollout 5G services that will empower smart devices, IoT. The new telecommunications infrastructure required to enable 5G will bring a huge leap in the available bandwidth. This will enable end-users (both machine and human) to experience much faster access and downloads, and share more data across more devices.

Along with the benefits and opportunities come new cybersecurity risks. For example, as more powerful smart devices come online, the networks hosting these devices will have an increased attack surface, which makes them bigger targets for DDoS attacks. It also increases the opportunity for those devices to be harnessed for the purposes of launching damaging DDoS attacks against other targets.

5G will power more virtual reality, artificial intelligence, remote surgery and automated machinery, all of which will rely on highly available and low latency connectivity. Downtime or service disruption for networks that support these critical applications will become increasingly disastrous (or, at the very least, much less tolerated).

Any organisation which relies on the Internet for its business, needs to be prepared for the increased cyber risks that 5G brings. In particular, Internet Service Providers now face a significant challenge, securing their increasingly complex and exponentially faster networks in an era where DDoS attacks have grown in frequency and sophistication. It will be critical that they prevent DDoS traffic from disrupting their own network-based service offerings, as well as those of their customers.

Super-scale DDoS protection

Carriers and other Tier-1 Service Providers have traditionally adopted a bifurcated approach to DDoS protection, for reasons of cost and the practicalities of deploying the available protection solutions. This two-tier service results in only the smaller DDoS attacks being filtered out, with larger attacks being addressed by blocking all traffic headed for the target, taking them offline for the duration. This may have been more accepted in the past but, as organisations increasingly rely on their internet presence being available 24/7, this presents an increasing challenge for the providers.

Recent advances in the inherent traffic filtering capabilities of network routers, from vendors such as Juniper Networks, is enabling a new generation of protection. Security solutions can now leverage next generation router filtering to deliver super-scale protection directly at the perimeter of a network.

We believe that Corero is the first DDoS vendor to effectively leverage real-time infrastructure-based traffic-filtering, which is enabling protection to be extended to an unprecedented tens-of-terabits scale. Combined with Corero's highly automated approach, providers can deliver this super-scale protection at a price-point that was not previously possible.

Strategy

Corero's focus is to scale its revenue by focusing on the following priorities:

1. Scaling the business towards profitability

- Three-pronged go-to-market focus:
    - Direct sales: Corero sales team focused on the SmartWall target market to leverage success to date
    - Indirect sales: channel partner proposition
    - Partner sales: close engagement with go-to-market partners such as Juniper and GTT Communications and development of additional relationships
- Channel leverage: Utilise Juniper channel partners given close alignment between Corero and Juniper's customer focus (service providers, cloud providers and digital enterprises)

2. Investment in sales and marketing to drive growth
    - Sales investment to support growth plans
    - Marketing spend focused on new customer sales lead generation

3. Maintaining competitive advantage
    - Incremental product enhancements with stable R&D investment
        - New DDoS attack defences
        - New machine learning and artificial intelligence capabilities

Outlook

Corero enters 2019 following a year of solid growth in revenue and order intake and with a significant resale partnership agreement in place with Juniper Networks. The Board is confident about Corero's prospects in the short to medium term, with the DDoS mitigation market fundamentals remaining strong and market analysts forecasting double digit growth. Corero remains well-placed to capitalise on the market opportunities and generate future growth.

[1] Recurring revenue comprises maintenance, support services and SaaS recognised revenue
[2] EBITDA loss is defined as loss before depreciation excluding DDoS protection as-a-service assets depreciation which is charged to cost of sales, amortisation, financing, tax and unrealised foreign exchange differences on an intercompany loan
[3] Restated as a result of a change in accounting policy related to the implementation of IFRS 15
[4] Adjusted operating costs is defined as costs before depreciation excluding DDoS protection as-a-service assets depreciation which is charged to cost of sales, amortisation, financing, tax and unrealised foreign exchange differences on an intercompany loan

Consolidated Statement of Comprehensive Income
for the year ended 31 December 2018

	Total 2018 $'000	Total 2017 Restated $'000
Revenue	9,951	8,531
Cost of sales	(2,188)	(2,126)
Gross profit	7,763	6,405
Operating expenses before highlighted items	(9,427)	(11,993)
Depreciation and amortisation of intangible assets	(3,300)	(2,938)
Operating expenses	(12,727)	(14,931)
Operating loss	(4,964)	(8,526)
Finance income	9	5
Finance costs	(268)	(4)
Loss before taxation	(5,223)	(8,525)
Taxation	-	116
Loss for the year	(5,223)	(8,409)
Other comprehensive expense		
Items that will or may be reclassified to profit and loss: Difference on translation of UK functional currency entities	(711)	805
Total comprehensive expense for the year	(5,934)	(7,604)
Total loss for the year attributable to:		
Equity holders of the parent	(5,223)	(8,409)
Total	(5,223)	(8,409)
Total comprehensive expense for the year attributable to:		
Equity holders of the parent	(5,934)	(7,604)
Total	(5,934)	(7,604)

Consolidated Statement of Financial Position
as at 31 December 2018

	2018 $'000	2017 Restated $'000
Assets		
Non-current assets		
Goodwill	8,991	8,991
Acquired intangible assets	14	37
Capitalised development expenditure	6,447	7,664
Property, plant and equipment	611	770
Trade and other receivables	227	76
	16,290	17,538
Current assets		
Inventories	125	94
Trade and other receivables	2,977	1,925
Cash and cash equivalents	8,026	1,365
	11,128	3,384
Liabilities		
Current Liabilities		
Trade and other payables	(1,799)	(1,305)
Borrowings	(849)	-
Deferred income	(2,034)	(1,702)
	(4,682)	(3,007)
Net current assets	6,446	377
Non-current liabilities		
Trade and other payables	(134)	-
Borrowings	(2,757)	-
Deferred income	(846)	(287)
	(3,737)	(287)
Net assets	18,999	17,628
Total equity attributable to owners of the parent		
Ordinary share capital	5,740	4,556
Capital redemption reserve	7,051	7,051
Share premium	79,338	73,239
Share options reserve	344	322
Translation reserve	(2,029)	(1,318)
Retained earnings	(71,445)	(66,222)
Total equity	18,999	17,628

Consolidated Statement of Cash Flow
for the year ended 31 December 2018

	2018 $'000	2017 Restated $'000
Loss for the year	(5,223)	(8,409)
Adjustments for non-cash movements:		
Amortisation of acquired intangible assets	23	55
Amortisation and impairment of capitalised development expenditure	2,918	2,408
Depreciation	483	548
Finance income	(9)	(5)
Finance expense	268	4
Taxation	-	(116)
Qualifying research and development expenditure tax credit	-	116
Share-based payment charge	22	21
Decrease in inventories and as-a-service-assets	100	127
Increase in trade and other receivables	(701)	(592)
Increase/(decrease) in payables	293	(201)
Net cash used in operating activities	(1,826)	(6,044)
Cash flows from investing activities		
Purchase of intangible assets	-	(10)
Capitalised development expenditure	(1,701)	(2,171)
Purchase of property, plant and equipment	(459)	(497)
Net cash used in investing activities	(2,160)	(2,678)
Cash flows from financing activities		
Net proceeds from issue of ordinary share capital	7,283	6,995
Finance income	9	5
Finance expense	(222)	(4)
Net proceeds from borrowings	3,938	-
Net cash from financing activities	11,008	6,996
Effects of exchange rates on cash and cash equivalents	(361)	151
Net increase/(decrease) in cash and cash equivalents	6,661	(1,575)
Cash and cash equivalents at 1 January	1,365	2,940
Cash and cash equivalents at 31 December	8,026	1,365

Consolidated Statement of Changes in Equity
for the year ended 31 December 2018

	Share capital $'000	Capital redemption reserve $'000	Share premium account $'000	Share options reserve $'000	Translation reserve $'000	Retained earnings $'000	Total attributable to equity holders of the parent $'000
1 January 2017 (as previously stated)	3,119	7,051	67,681	301	(2,123)	(57,813)	18,216
Prior year adjustment – IFRS 15 Revenue from Contracts with Customers	-	-	-	-	-	164	164
1 January 2017 (as restated)	3,119	7,051	67,681	301	(2,123)	(57,649)	18,380
Loss for the year	–	–	–	–	–	(8,573)	(8,573)
Other comprehensive income	–	–	–	–	805	-	805
Total comprehensive expense for the year (as restated)	–	–	–	–	805	(8,573)	(7,768)
Contributions by and distributions to owners							
Share-based payments	–	–	–	21	–	–	21
Issue of share capital	1,437	–	5,558	–	–	–	6,995
Total contributions by and distributions to owners	1,437	–	5,558	21	–	–	7,016
31 December 2017 and 1 January 2018 (as restated)	4,556	7,051	73,239	322	(1,318)	(66,222)	17,628
Loss for the year	–	–	–	–	–	(5,223)	(5,223)
Other comprehensive loss	–	–	–	–	(711)	–	(711)
Total comprehensive expense for the year	–	–	–	–	(711)	(5,223)	(5,934)
Contributions by and distributions to owners							
Share-based payments	–	–	–	22	–	–	22
Issue of share capital	1,184	–	6,099	–	–	–	7,283
Total contributions by and distributions to owners	1,184	–	6,099	22	–	–	7,305
31 December 2018	5,740	7,051	79,338	344	(2,029)	(71,445)	18,999

1. General information

These consolidated financial statements are presented in US Dollars ("$") which represents the presentation currency of the Group. The average $-GBP sterling ("GBP") exchange rate, used for the conversion of the statement of comprehensive income, for the 12 months ended 31 December 2018 was 1.33 (2017: 1.29). The closing $-GBP exchange rate, used for the conversion of the Group's assets and liabilities, at 31 December 2018 was 1.28 (2017: 1.35).

The principal accounting policies adopted in the preparation of the financial information in this results announcement are consistent with those that the company has applied in its financial statements for the year ended 31 December 2017 apart from new standards which give rise to a change in the Group's accounting policies comprising IFRS 9 Financial Instruments and IFRS 15 Revenue from Contracts with Customers.

The financial information set out above does not constitute the Company's Annual Report and Accounts for the year ended 31 December 2018. The Annual Report and Accounts for 2017 have been delivered to the Registrar of Companies and those for 2018 will be delivered shortly. The auditor's report for the Company's 2018 Annual Report and Accounts was unqualified but did draw attention to the material uncertainty relating to going concern.

The Directors have prepared detailed income statement, balance sheet and cash flow projections for the period to 31 December 2020. The cash flow projections have been subjected to sensitivity analysis at the revenue, cost and combined revenue and cost levels. The cash flow projections show that the Group and Company will maintain a positive cash balance until at least December 2020. In addition, the projections and sensitivity analyses confirm that the bank loan covenants will be met for a period of at least 12 months from the date of approval of these financial statements.

On this basis, the Directors have therefore concluded that it is appropriate to prepare the financial statements on a going concern basis.

However, the ability of the Company and Group to achieve the future profit and cash flow projections cannot be predicted with certainty. Failure of the Company and the Group to meet these projections and deliver revenue growth may adversely impact the achievability of the bank loan covenants which may result in the bank loan being required to be repaid before the maturity date if the revenue covenants are not met and cannot be renegotiated. This would adversely impact the Company and the Group's working capital position and would require the Company to raise additional funding, with no guarantee such funding would be secured.

Taken together, the achievability of the projections and availability of additional funding if required indicate a material uncertainty that may cast significant doubt on the Group's ability to continue as a going concern for the foreseeable future.

The financial statements do not include the adjustments that would result if the Group and Company was unable to continue as a going concern.

The auditor's report did not contain statements under s498(2) or (3) of the Companies Act 2006.

Whilst the financial information included in this results announcement has been computed in accordance with International Financial Reporting Standards (IFRSs) this announcement does not itself contain sufficient information to comply with IFRSs.

The Annual Report and Accounts for the year ended 31 December 2018 are available on the Company's website www.corero.com/investors.

The information in this results announcement was approved by the board on 10 April 2019.