Interim Report & Accounts 2017

Corero Network Security plc

Corero Network Security is the leader in real-time, high-performance DDoS defence solutions.

Service providers, hosting providers and digital enterprises rely on Corero's award winning SmartWall technology to eliminate the DDoS threat to their environment through automatic attack detection and mitigation, coupled with complete network visibility, analytics and reporting.

What is a DDoS attack?

A Distributed Denial of Service (DDoS) attack is a cyber threat, in which multiple compromised computer systems attack a target, such as a server, website or other network asset, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system, forces it to slow down or shut down, thereby denying service to legitimate users or systems. DDoS attacks are a threat to service availability, network security, brand reputation and ultimately lead to lost revenues.

Attackers are continuing to leverage DDoS attacks as part of their cyber threat arsenal to either disrupt business operations or access sensitive corporate information, and they are doing it in increasingly creative ways that circumvent traditional security solutions or nullify the previous effectiveness of DDoS scrubbing centres.

Market demand

Underlying market demand is being driven by the increasing number and severity of DDoS attacks. In Q1 2017:

- Corero customers experienced an average of 124 attacks per month, an increase of 9% compared to Q4 2016.
- The average size of these attacks increased, with a 55% increase in attacks over 10Gbps.
- 71% of DDoS attacks lasted less than 10 minutes (with attackers targeting short duration damaging attacks to avoid traditional detection methods).

4x Attacks per day

71% 10 Minutes or Less

80% Less than 1Gbps

DDoS attacks continue to be frequent, short duration and low in volume*

Akamai, in their State of the Internet Security Report for Q1 2017 reported a 30% increase in DDoS attacks over Q1 2016.

*Source: Corero Q1 2017 DDoS Trends and Analysis

Contents

Discover more online at:
www.corero.com/investors/

Highlights

Strong new customer acquisition and continued SmartWall order momentum

Financial Highlights

SmartWall revenue up

51%

over H1 2016 to $4.4 million

- Reduction in legacy products revenue as expected to $0.4 million (H1 2016: $1.9m)
- Overall revenue of $4.8 million (H1 2016: $4.8 million)
- 177% growth in recurring SmartWall revenue over H1 2016

EBITDA loss

$3.4m

(H1 2016: loss $2.5 million)

- Includes an unrealized foreign exchange loss of $0.3m on an intercompany loan (H1 2016: gain $0.8m)

Loss before tax

$4.8m

(H1 2016: $4.1 million)

Loss per share

2.0c

(H1 2016: 2.4 cents)

Net Cash

$5.1m

at 30 June 2017
(30 June 2016: $8.7 million)

Operating Highlights

- Strong new customer acquisition
  - 13 new customers added (H1 2016: 12)
  - First $1 million customer
  - New Tier 1 service provider customer signed (GTT Communications, Inc)
- Continued SmartWall order momentum
  - Order intake up 41% to $4.8 million (H1 2016: $3.4 million)
  - Follow-on orders from existing customers $1.4 million (H1 2016: $0.3 million)
- 7 new as-a-Service customers (H1 2016: nil)
- Expanded SmartWall solution offering to 100Gbps (from current 10Gbps)
- Signed technology partnerships with Gigamon, Juniper Networks and McAfee

Full Year Trading Update

Based on progress in the first half of the year and strong pipeline of opportunities, the Board is positive about the future prospects for the Company and that the results for the year ending 31 December 2017 are expected to be in-line with market expectations.

"Corero has made good progress in the first half of 2017 with several significant milestones including our first $1 million customer, a continued increase in recurring revenues, expansion of our product line to 100Gbps capability and the launch of a virtual appliance, software only DDoS mitigation solution."

"We continue to win customers in our target markets of service and hosting providers and digital enterprises, almost doubling the number of SmartWall customers in the past 12 months to some 80 customers at the end of June 2017. In addition, our focus on increasing our routes to market through partnerships has resulted in formal agreements with Gigamon, Juniper Networks and McAfee. We expect the benefits of these and other such relationships we are pursuing to contribute in the second half of 2017."

Ashley Stephenson

CEO

Interim results

for the six month period ended 30 June 2017

Corero continues to win customers in its target markets of service and hosting providers and digital enterprises, almost doubling the number of SmartWall customers in the past 12 months to some 80 customers at the end of June 2017.

H1 2017 was a period of significant progress for Corero

While overall revenue was flat on H1 2016, sales of our SmartWall product to service and hosting providers and digital enterprises grew strongly (up 51% over H1 2016), providing further validation of the Company's innovative IP and the growing market opportunity.

From a relatively stable cost base, management remains focused on scaling up SmartWall revenue as a means to achieving profitability. The Company continued to make good progress to this end in the first half, reaching a number of milestones including the signing of its first $1 million customer, an increase of more than $1 million in follow-on revenue from existing customers, 96% support contract renewal rate and the addition of a new Tier 1 customer in GTT Communications, Inc.

The first half also saw encouraging uptake of the Company's subscription-based as-a-Service model, with seven new customers signing service contracts. Launched in Q4 of 2016 to complement the Company's perpetual license offering, the model reduces revenue recognised at the time of the initial customer order but increases the contract value and recurring revenue over the life of the deal. The cash profile of as-a-Service sales is typically monthly payments.

The period also saw Corero begin executing on its strategy of accelerating revenue growth by recruiting go-to-market technology partners such as Juniper Networks and entering into revenue share agreements with customers that repackage Corero's service as their own offering.

In January, Corero strengthened its sales leadership with the appointment of Andrew Lloyd as President and EVP Sales & Marketing, a proven sales leader with over 25 years' experience in the IT software industry.

The loss for the period reflects the continuing investment in technology and IP resulting in the launch in first half of 2017 of its SmartWall 100G product and the development of a virtual appliance version of the SmartWall product which is expected to open up OEM licensing and re-sale opportunities. Corero is targeting continued sales growth which with 70% plus gross margins is expected to result in improved profitability and targeted EBITDA break-even in the final quarter of 2017.

In April, the Company completed a placing and subscription to raise $7.0 million (after costs) to support SmartWall sales and marketing activities in the US and Europe, for further development of the SmartWall product and for general working capital requirements.

Financial Summary

In the six months to 30 June 2017, Corero reported revenue of $4.8 million (H1 2016: $4.8 million) and an EBITDA loss of $3.4 million (H1 2016: loss $2.5 million). SmartWall revenue grew 51% over H1 2016 (67% over H2 2016). As expected, revenue from legacy products reduced to $0.4 million (H1 2016: $1.9m).

Operating expenses net of capitalised R&D were $6.9 million (H1 2015: $6.3 million). Included in operating expenses was an unrealised exchange loss on an intercompany loan of $0.3m (H1 2016: gain $0.8 million) arising on an intercompany loan. Capitalised R&D costs were $1.3 million (H1 2016: $1.5 million). Total operating costs excluding the unrealised exchange loss of $0.3 million were $8.0 million, which was lower than the comparable period of $8.6 million on a like-for-like basis excluding the unrealised foreign exchange gain of $0.8 million.

The loss before taxation was $4.8 million (H1 2016: loss $4.1 million) including amortisation of capitalised R&D of $1.1 million (H1 2016: $1.1 million) and amortisation of acquired intangible software assets $0.03 million (H1 2016: $0.2 million). The reported loss per share was 2.0 cents (H1 2016: 2.4 cents).

Corero had cash of $5.1 million at 30 June 2017 (2016: $8.7 million), having raised $7.0 million net of costs in April 2017. The Company had no debt at 30 June 2017 (H1 2016: $nil). The net reduction in cash from operating activities in the 6 months ended 30 June 2017 was $3.7 million (H1 2016: net reduction $2.0 million) reflecting the loss for the period and increased in working capital investment in the period of $0.3 million (H1 2016: working capital reduction of $0.4 million).

DDoS Attacks are Accelerating in Complexity, Scale and Frequency

Today's DDoS attacks are almost unrecognisable from the early days of attacks, when most were simple, volumetric attacks intended to cause embarrassment and brief disruption. Today, the motives behind attacks are increasingly to support criminal activity, the techniques are becoming ever-more complex and the frequency of attacks is growing significantly. This is particularly true in light of automated attacks, which allow attackers to switch vectors faster than any human or traditional IT security solution can respond.

51%
SmartWall revenue growth

177%
recurring SmartWall revenue over H1 2016

96%
Support contract renewal rate

The combination of the size, frequency and duration of modern attacks represents a serious security and availability challenge for Internet providers and users. Minutes or even tens of minutes of downtime or latency significantly impacts the delivery of essential services. When you combine these factors, victims are faced with a significant security and availability challenge.

Beyond the ability to deny service, DDoS attacks have become a tool in 'denial of security', by acting as camouflage or a distraction mechanism to mask more threatening activities – usually data theft and network infiltration.

These attacks act as a smokescreen to distract IT and security teams from the real breach that's taking place, which could see data being exfiltrated, networks being mapped for vulnerabilities, or a whole host of other potential risks manifesting themselves. There have been data breaches reported over the last few years that indicate DDoS attacks have been occurring simultaneously, as a component of a wider strategy; meaning hackers are utilizing the DDoS technique in a significant way.

To keep up with the growing sophistication and organisation of well-equipped and well-funded threat actors, it is essential that organisations maintain comprehensive visibility across their networks to instantly and automatically detect and block any potential DDoS incursions as they arise. Proactive DDoS protection is a critical element in proper cyber security protection against loss of service and data breach activity. This level of protection cannot be achieved with traditional Internet Gateway security solutions such as firewalls, IPS and the like.

The only proper defence is to use an automatic, always-on DDoS mitigation system, which can monitor all traffic in real-time, negate the flood of attack traffic at the internet edge, eliminate service outages and allow security personnel to focus on uncovering any subsequent malicious activity, such as data breaches or malware deposits.

This type of always-on protection can come in various forms – either on-premises, or purchased as a security service from an upstream provider. It is only through deploying these real-time solutions such as SmartWall that organisations will be able to identify and mitigate the most serious DDoS attacks on their networks in the years ahead.

Strong Market Drivers

Underlying market demand is being driven by the increasing number and severity of DDoS attacks. In Q1 2017:

- Corero customers experienced an average of 4 attacks per day or 124 attacks per month, an increase of 9% compared to Q4 2016.
- The average size of these attacks increased, with a 55% increase in attacks over 10Gbps.
- 71% of DDoS attacks lasted less than 10 minutes (with attackers targeting short duration damaging attacks to avoid traditional detection methods).

Akamai, in their State of the Internet Security Report for Q1 2017, reported a 30% increase in DDoS attacks over Q1 2016.

Corero is targeting a high growth security market; the market for DDoS prevention appliances is forecast by IHS Technology, a leading industry analyst, to reach more than $1.0 billion by 2020 with a CAGR of 11.0% in the period 2016 to 2020. This growth is driven by a growing awareness of the threat of DDoS attacks and the increased focus and resourcing of governments (most notably in the US and UK) on national security strategies and policies on cyber security.

Additional Market Segment

The increase in DDoS attacks, increasing board room awareness and new cyber security regulatory requirements such as the European NIS Directive and General Data Protection Regulation, has opened up an opportunity for Corero to extend its sales focus beyond service and hosting providers to online digital enterprises. These enterprises increasingly understand the benefit of using the real-time protection offered by products such as SmartWall to complement the on-demand protection generally offered by service providers. Corero has to date secured two $1 million plus contracts from online digital enterprises and expects them to be an important market going forwards.

Outlook

Corero is well positioned to be a major disrupter in the DDoS protection market and leader in delivering real-time DDoS mitigation. The Company has innovative, award winning IP (validated by over 100 installations and a leading independent third party testing company), a strong go-to-market model and growing recurring revenues. Underlying market demand is being driven by the increasing number and severity of DDoS attacks and increasing awareness of the threat of cyber attacks as a result of high profile attacks such as the crippling DDoS attack on Dyn in 2016 and recent WannaCry ransomware attacks.

Based on progress in the first half of the year and strong pipeline of opportunities, the Board is positive about the future prospects for the Company and that results for the year ending 31 December 2017 are expected to be in-line with market expectations.

Consolidated Interim Statement of Comprehensive Income

for the six month period ended 30 June 2017

	Unaudited six months ended 30 June 2017 $'000	Unaudited six months ended 30 June 2016 $'000	Audited year ended 31 December 2016 $'000
Revenue	4,813	4,791	8,772
Cost of sales	(1,275)	(1,002)	(2,071)
Gross profit	3,538	3,789	6,701
Operating expenses before highlighted items	(6,935)	(6,274)	(11,847)
Depreciation and amortisation of fixed assets	(1,359)	(1,601)	(3,128)
Impairment of goodwill	–	–	(8,992)
Operating expenses	(8,294)	(7,875)	(23,967)
Operating loss	(4,756)	(4,086)	(17,266)
Finance income	3	4	9
Finance costs	(4)	(6)	(6)
Loss before taxation	(4,757)	(4,088)	(17,263)
Taxation	–	68	85
Loss for the period	(4,757)	(4,020)	(17,178)
Other comprehensive expense			
Difference on translation of UK functional currency entities	452	(1,533)	(2,355)
Total comprehensive expense for the period	(4,305)	(5,553)	(19,533)
Total loss for the period attributable to:			
Equity holders of the parent	(4,757)	(4,020)	(17,178)
Total	(4,757)	(4,020)	(17,178)
Total comprehensive expense for the period attributable to:			
Equity holders of the parent	(4,305)	(5,553)	(19,533)
Total	(4,305)	(5,553)	(19,533)

Basic and diluted loss per share	30 June 2017 Cents	30 June 2016 Cents	31 December 2016 Cents
Basic and diluted loss per share	(2.0)	(2.4)	(9.0)

Consolidated Interim Statement of Financial Position

as at 30 June 2017

	Unaudited as at 30 June 2017 $'000	Unaudited as at 30 June 2016 $'000	Audited as at 31 December 2016 $'000
Assets			
Non-current assets			
Goodwill	8,991	17,983	8,991
Acquired intangible assets	50	139	82
Capitalised development expenditure	8,074	8,056	7,901
Property, plant and equipment	1,070	882	970
	18,185	27,060	17,944
Current assets			
Inventories	112	641	65
Trade and other receivables	2,081	2,350	2,307
Cash and cash equivalents	5,118	8,693	2,940
	7,311	11,684	5,312
Liabilities			
Current Liabilities			
Trade and other payables	(1,611)	(2,346)	(1,728)
Deferred income	(2,581)	(3,043)	(2,457)
	(4,192)	(5,389)	(4,185)
Net current assets	3,119	6,295	1,127
Non-current liabilities			
Deferred income	(398)	(1,162)	(855)
Deferred taxation	–	(17)	–
	(398)	(1,179)	(855)
Net assets	20,906	32,176	18,216
Equity			
Ordinary share capital	4,556	3,119	3,119
Capital redemption reserve	7,051	7,051	7,051
Share premium	73,239	67,680	67,681
Share options reserve	301	282	301
Translation reserve	(1,671)	(1,301)	(2,123)
Retained earnings	(62,570)	(44,655)	(57,813)
Total equity	20,906	32,176	18,216

Consolidated Interim Statement of Cash Flows

for the six month period ended 30 June 2017

	Unaudited six months ended 30 June 2017 $'000	Unaudited six months ended 30 June 2016 $'000	Audited year ended 31 December 2016 $'000
Cash flows from operating activities			
Loss for the period	(4,757)	(4,020)	(17,178)
Adjustments for:			
Amortisation of acquired intangible assets	32	239	325
Impairment loss on intangible assets	–	–	8,992
Amortisation of capitalised development expenditure	1,085	1,074	2,252
Depreciation	260	288	551
Loss on sale of property, plant and equipment	–	–	9
Finance income	(3)	(4)	(9)
Finance expense	4	6	6
Taxation	–	(68)	(85)
Share based payment charge	–	–	19
(Increase)/decrease in inventories	(47)	20	596
Decrease in trade and other receivables	242	1,585	1,605
Decrease in payables	(481)	(1,160)	(2,623)
Net cash used in operating activities	(3,665)	(2,040)	(5,540)
Cash flows from investing activities			
Purchase of intangible assets	–	(3)	(32)
Capitalised development expenditure	(1,258)	(1,510)	(2,533)
Purchase of property, plant and equipment	(353)	(277)	(644)
Net cash used in investing activities	(1,611)	(1,790)	(3,209)
Cash flows from financing activities			
Net proceeds from issue of ordinary share capital	6,995	11,391	11,392
Finance income	3	4	9
Finance expense	(4)	(6)	(6)
Net cash from financing activities	6,994	11,389	11,395
Effects of exchange rates on cash and cash equivalents	460	(1,572)	(2,412)
Net increase in cash and cash equivalents	2,178	5,987	234
Cash and cash equivalents at 1 January	2,940	2,706	2,706
Cash and cash equivalents at balance sheet dates	5,118	8,693	2,940

Consolidated Interim Statement of Changes in Equity

for the six month period ended 30 June 2017

	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 2016	2,573	7,051	56,835	282	232	(40,635)	26,338
Loss for the period	–	–	–	–	–	(4,020)	(4,020)
Other comprehensive expense	–	–	–	–	(1,533)	–	(1,533)
Total comprehensive expense for the period	–	–	–	–	(1,533)	(4,020)	(5,553)
Contributions by and distributions to owners							
Issue of share capital	546	–	10,845	–	–	–	11,391
Total contributions by and distributions to owners	546	–	10,845	–	–	–	11,391
30 June 2016	3,119	7,051	67,680	282	(1,301)	(44,655)	32,176
Loss for the period	–	–	–	–	–	(13,158)	(13,158)
Other comprehensive expense	–	–	–	–	(822)	–	(822)
Total comprehensive expense for the period	–	–	–	–	(822)	(13,158)	(13,980)
Contributions by and distributions to owners							
Share based payments	–	–	–	19	–	–	19
Issue of share capital	–	–	1	–	–	–	1
Total contributions by and distributions to owners	–	–	1	19	–	–	20
31 December 2016 and 1 January 2017	3,119	7,051	67,681	301	(2,123)	(57,813)	18,216
Loss for the period	–	–	–	–	–	(4,757)	(4,757)
Other comprehensive expense	–	–	–	–	452	–	452
Total comprehensive expense for the period	–	–	–	–	452	(4,757)	(4,305)
Contributions by and distributions to owners							
Issue of share capital	1,437	–	5,558	–	–	–	6,995
Total contributions by and distributions to owners	1,437	–	5,558	–	–	–	6,995
30 June 2017	4,556	7,051	73,239	301	(1,671)	(62,570)	20,906

Notes to the interim financial statements

1. General information and basis of preparation

Corero Network Security plc (the "Company") is a company domiciled in England. The condensed consolidated interim financial statements of the Company for the six months ended 30 June 2017 comprise the Company and its subsidiaries (together referred to as the "Group").

These condensed consolidated financial statements have been prepared in accordance with IAS 34, "Interim Financial Reporting", as adopted by the European Union. They do not include all disclosures that would otherwise be required in a complete set of financial statements and should be read in conjunction with the 2016 Annual Report. The financial information for the half years ended 30 June 2017 and 30 June 2016 does not constitute statutory accounts within the meaning of Section 434(3) of the Companies Act 2006 and has neither been audited or reviewed.

The annual financial statements of Corero Network Security plc are prepared in accordance with IFRSs as adopted by the European Union. The comparative financial information for the year ended 31 December 2016 included within this report does not constitute the full statutory accounts for that period. The statutory Annual Report and Financial Statements for 2016 have been filed with the Registrar of Companies. The Independent Auditors' Report on that Annual Report and Financial Statement for 2016 was unqualified, did not draw attention to any matters by way of emphasis, and did not contain a statement under 498(2) or 498(3) of the Companies Act 2006.

The consolidated financial statements have been prepared on a going concern basis as the Directors believe that the current sales prospects, combined with existing working capital resources should ensure that the Group has adequate working capital to service its existing business for the foreseeable future. The directors have made this assessment based on internal forecasts and cash flow projections.

These consolidated interim financial statements were approved by the Board on 13 September 2017 and approved for issue on 14 September 2017.

2. Loss per share

Loss per share is calculated by dividing the earnings attributable to ordinary shareholders by the weighted average number of ordinary shares in issue during the period.

At the reporting dates there were no potentially dilutive ordinary shares. Therefore the diluted loss per share is equal to the loss per share.

	30 June 2017			30 June 2016		
	Loss $'000	Weighted average number of 1p shares Thousand	Loss per share Cents	Loss $'000	Weighted average number of 1p shares Thousand	Loss per share Cents
Basic and diluted loss per share	(4,757)	243,922	(2.0)	(4,020)	168,276	(2.4)

	31 December 2016		
	Loss $'000	Weighted average number of 1p shares Thousand	Loss per share Cents
Basic and diluted loss per share	(17,178)	189,959	(9.0)

Corporate Directory

Directors

Jens Montanana (Non-Executive Chairman)
Ashley Stephenson (CEO)
Andrew Lloyd (President and EVP Sales & Marketing)
Andrew Miller (CFO)
Richard Last (Non-Executive Director)

Secretary and Registered Office

Duncan Swallow
Regus House
Highbridge
Oxford Road
Uxbridge
Middlesex
UB8 1HR

Nominated Adviser and Broker

Cenkos Securities plc
6.7.8 Tokenhouse Yard
London
EC2R 7AS

Auditor

BDO LLP
55 Baker Street
London
W1U 7EU

Solicitors

Dorsey and Whitney LLP
199 Bishopsgate
London
EC2M 3UT

Bankers

Santander
2 The Forbury
Reading
RG1 3EU

Square 1 Bank
406 Blackwell Street
Suite 240
Durham
North Carolina
27701
USA

Registrars

Capita Asset Services
The Registry
34 Beckenham Road
Beckenham
Kent
BR3 4TU

Website address

www.corero.com

Registered Office
Regus House
Highbridge
Oxford Road
Uxbridge
Middlesex
UB8 1HR