

20 November 2014

Company Announcements Office
Australian Securities Exchange Limited
Level 6
20 Bridge Street
Sydney NSW 2000

Dear Sir/Madam

SENETAS CORPORATION – 2014 ANNUAL GENERAL MEETING

We attach a copy of the Chairman's address and the CEO's presentation to be delivered to shareholders at the Senetas Corporation Limited Annual General Meeting to be held at Bayview on the Park Hotel, Lakeside Room 1, 52 Queens Road, Melbourne on Thursday, 20 November 2014 at 10:30 am (Melbourne time).

Yours sincerely



Brendan Case
Company Secretary



SENETAS CORPORATION LIMITED AGM

CHAIRMAN'S OPENING ADDRESS

20 NOVEMBER 2014

Good morning ladies and gentlemen. Welcome to the Senetas Corporation Limited 2014 annual general meeting.

It is now 10.30am, and this is a properly constituted meeting and a quorum is present. I therefore declare this Annual General Meeting of Senetas Corporation Limited open.

Thank you for your interest and attendance today.

INTRODUCTION

I will begin by introducing our board of directors. On my left is our CEO, Andrew Wilson, whom I thank for his leadership during the past financial year. Next to Andrew is Lachie Given, a non-executive director; and on the far left is retired Lieutenant General Ken Gillespie, also a non-executive director. And our company secretary is Brendan Case.

I thank Ken and Lachie for their valuable input during the past financial year. They are readily available to assist our company's efforts to grow and their contributions have been important to our success. We're also grateful to Brendan for his excellent services to the board and company.

That brings me to the Senetas employees, whom I must also thank for their capabilities and tireless efforts during the year. In particular I thank the senior management team - Julian Fay - CTO; John Weston - Engineering Director; Barb McMeekin - CFO; and Simon Galbally - Marketing Director.

We have achieved a great deal during the last financial year and feel we have now entered the next phase of Senetas's growth. Although we have been very successful from where we re-started the business 2 years ago; your board of directors believes we have only just commenced the business's revival. There is more to be done - there are significant opportunities as well as challenges.

Today, my message in my capacity as chairman of the board of directors, to all Senetas investors is quite simple. Our objectives as a board are to help ensure the business continues to improve the way things are done and leverage the successes achieved; seize the opportunities and address the challenges we have identified; and continue pushing growth in our core business of certified hardware encryption products, and our expertise in high-speed electronics engineering.

I am sure your board of directors is up to these aspirations and our role of guiding management.



To this end, the company has already commenced development of a 100 gigabit per second encryptor to meet identified future customer requirements. Further, our talented engineering team has commenced development of a platform that may be utilised for 'bespoke' encryptor customer orders - tailored to specific and unique customer and foreign market needs.

We will continue maintaining our commitment to independent international government testing authority certifications, which so well differentiate Senetas products in an increasingly competitive environment. This is clearly shown to our global markets by the recent and significant achievement of NATO certification. This certification itself provides us with increased opportunities. Certifications also differentiate Senetas encryptors from recently exposed 'open systems' vulnerabilities that have drawn significant market attention and concern. Obviously, our products are not exposed to such vulnerabilities!

We continue our focus on product enhancements and updates, which increase their value proposition and benefits to our customers. Our R&D roadmap seeks opportunities to deliver continuing advancements and customer benefits. For example, we recently introduced the TRANSEC – transmission security - feature, which allows customers to 'hide' their network traffic patterns from eavesdropping.

Importantly, the board and management are pursuing new and innovative products that leverage Senetas core skills. We are also seeking acquisition opportunities that similarly leverage Senetas core expertise and technical skills, as well as add substantial value to our overall business.



THEME

Last year, when presenting to you, I referred to a number of risks associated with cyber-security and the increasing cyber-attacks conducted around the world. Today, these risks are not just continuing, but their frequency and the damage caused are growing.

The information security warnings, repeatedly issued by revered cyber-security experts and government security agencies alike, have been proven correct. However, during 2014 we continue to see examples of organisations that not only suffer serious information breaches; but the data in the hands of unauthorised parties is too often unencrypted!

Those breaches would not have damaged the organisations' reputations had the information been encrypted!

Moreover, there is no indication that this risk pattern has flattened or slowed down. Conversely, and globally, the expectation is that this pattern will continue to increase, just as the volumes of data created and transmitted also continue to increase.

Understanding this cyber-security pattern and the very real issues it raises; I would like to share with you, both a disturbing trend and a related conundrum, which poses something of a challenge for us. And I believe we have an answer, which also provides us further opportunities!

Western governments spend a lot of time and energy espousing the risks to cyber-security and national security alike - of cyber-terrorism, cyber-crime and rogue-state cyber-activities. They also comment endlessly about the need to ensure governments and industry adequately protect themselves and their information from cyber-threats.

However, the truth is that many western governments actually do little to effectively protect their data. Or, put more fairly, many governments do as little as possible to effectively protect their data!

Here we see the difference between 'rhetoric' and 'commitment'. There is certainly a lot of talk; but, when organisations are not encrypting sensitive data, we see a lack of commitment to information security.

Worryingly, in some cases, western governments' agencies take steps to ensure they do not 'have to' protect their data. These agencies have 'conveniently' satisfied themselves that their data - which often includes information-rich citizen information as well as government secrets, such as plans and decisions - is safe, although the information itself is not protected - not encrypted.

Such government agencies are able to achieve this 'convenient' position simply by 'manipulating' their data protection guidelines, standards and classifications, which they and their security advisers developed. They achieve this by either adjusting data sensitivity classifications; adjusting security requirements; or, by providing 'interpretative flexibility'.



Either way, the effect is to avoid encrypting the data – avoiding the most effective information security technique available! Ultimately, the effect is to leave the unencrypted information-rich data exposed to successful cyber-attacks and resulting breaches.

Government agencies' 'flexible interpretation' of information security guidelines result in allowing these agencies to 'take a punt' on information security – through their subjective judgments. For example, agencies may decide that their transmitted data is 'safe enough' because it is transmitted across fibre optic networks they or their government own and therefore it will not be breached. This occurs despite the obvious fact that 'ownership' of networks has absolutely nothing to do with information security and risks!

Such self-serving behaviours in the government sector are clearly driven by 'convenience' (financial or otherwise) – leading to scenarios such as adjusting the guidelines to suit an agency's purpose; and allowing an agency's subjective 'interpretation' of its own government's information security guidelines - simply its own specific agenda.

The key point is that, only when information is robustly encrypted to a certified standard, can the information be said to be protected. Only then is the information itself secure! Only encryption protects the information itself from successful information security breaches, making it useless in unauthorised hands. Therefore, this behaviour to avoid a requirement to encrypt information is simply risky and unacceptable!

Senetas and our partners around the world have seen evidence of such risky government agency behaviour.

Too many cyber-attacks - against both western government and major commercial organisations - have resulted in successful breaches where the information was unencrypted. Consequently, unnecessary harm has been caused by failures to encrypt information.

The real issue is that because the data itself was not protected - was not encrypted - the impact on citizens and customers alike may be very serious and long term – such as identity theft, which is a 'perfect' asset to terrorists and criminals alike!

And, before anyone doubts that risk, consider the recent US income tax example (reported by 60 Minutes USA) where through stolen identities, criminals pre-lodged thousands of citizens' income tax returns – receiving the refund into nominated bank accounts. The taxpayers only discovered this much later when upon lodging their legitimate returns, they received a reply: "Your tax return has already been lodged and tax refund paid into your nominated account"!

Moreover, and closer to home, if identity data was robustly encrypted throughout government and corporations handling sensitive identity information; would so many of the doomed passengers on board Malaysia Airlines flight ML370 have been discovered to have been carrying false passports?!



While cyber-attacks and successful breaches will likely continue to be every-day realities, the shocking issue is that the resulting devastating impact of successful breaches need not occur. If the data were encrypted there would not be any impact. The cyber-criminals would only obtain meaningless bits and bytes of encrypted data.

Instead - and it will be many years before anyone will know the full impact of these successful data breaches - the data stolen from western governments and commercial organisations may include citizen identities; government decision documentation; financial records; critical commercial intellectual property...and the list goes on. In many instances the culprits have been identified as being located in non-western states.

Now I come to the conundrum itself. Non-western governments and commercial organisations well recognise the risks associated with data transmitted across data networks and the risks of data theft, eavesdropping and data-corruption if the data is not encrypted.

Data security analysts have commented that they suspect - and I must say that the company and I are not expressing a specific view here - that western cryptographic algorithms may be to blame to some degree. So it seems that this is where non-western government and commercial organisations appear to prefer to adopt their own cryptographic algorithms - to, in their view, more effectively protect their data.

And now to the answer I believe we have. Today, Senetas and our partners are seeing evidence of a growing demand by non-western governments and commercial organisations for non-western cryptographic algorithms. Therefore, with our partners we have decided to target this market.

Those among you here today who are familiar with our encryption hardware and firmware technology will be aware that our unique products lend themselves to the implementation of 'custom algorithms'. This is a feature and benefit well promoted in our product collateral.

I am pleased to add that since identifying this custom algorithm opportunity, we are well advanced in our negotiations for our first product development project with a large non-western customer and market opportunity. We believe that this provides a growth opportunity through a new and growing market. Of course, we strive to be the first entrant and quickly establish our superior product credentials.

I am sure that you will all see the clear irony in the fact that while various western countries make a great deal of noise about serious information and national security risks; non-western countries say little, but act. They recognise that in addition to prevention and protection technologies, the data itself must be protected - the data must be encrypted before it may be considered protected.



In closing allow me to repeat what I said at last year's AGM - the risks of information theft; privacy breaches and other malicious attacks while it is transmitted across data networks cannot be overstated. As the use of data networks continues to grow exponentially due to technologies such as Cloud Computing, Big Data and Data centre services; data network breaches are inevitable. Information security is a process of 'catch-up' making encryption the ultimate protection against a successful breach.

Robust data protection through encryption is no longer an IT department issue alone. It is a critical part of the much bigger business planning topic that is an organisation-wide issue. It demands the attention of organisations' most senior management.

Therefore, failures by governments to effectively regulate and protect citizen information and government secrets by encrypting it, expose citizens and business to serious long-term risks. Similarly, business organisations that do not encrypt their data as it is transmitted from one place to another, also expose their customers, shareholders, suppliers, partners and employees to unacceptable risks.

Our own research into major corporations' readiness to comply with changes to the Australian Privacy Act – including penalties of up to \$1.3m for a single data breach - disturbingly revealed that more than 75% of interviewed organisations did not believe they were ready to comply. And none were concerned about the heavy financial penalties. It seemed the only concern shared among the interviewees was the likelihood of mandatory breach notification laws.

The international media have reported growing evidence that organisations that do not protect data from successful breaches – through encryption – will suffer catastrophic brand damage and customer, supplier and partner defection. Even those who do not suffer successful breaches will soon become uncompetitive – customers choosing to not take the risk!

###



SENETAS CORPORATION

CEO's PRESENTATION

ANNUAL GENERAL MEETING 2014

AGENDA

1. Introduction
2. Financial Performance and go to Market Model
3. Technology and Roadmap
4. Summary

1.0 | INTRODUCTION

SENETAS CORPORATION

ASX: SEN	Market Cap. (\$0.05 share): Revenue: EBITDA: Net Profit: Net Cash 20/11/14:	\$48 mill \$11.0 mill \$2.7 mill \$2.9 mill \$10.0 mill
Capital Structure	<ul style="list-style-type: none"> • Shares on Issue: 1,065 m • No. shareholders: 4900 	
Overview	<ul style="list-style-type: none"> • Head office in Melbourne, Australia • Products deployed across 29 countries • Growing demand for encryption solutions • Blue chip customer base • 40 employees • Offices in Melbourne Sydney and UK 	
Mission	<ul style="list-style-type: none"> • Excellent innovative R&D • Leverage world wide SafeNet relationship to build pipeline and revenue • Enter new markets (near-term focus is Eastern Europe & 100G encryption market) 	

SHARE PRICE PERFORMANCE

SENETAS FPO

■ SEN.AX

17 Nov, 2014



WHAT IS ENCRYPTION?



ENCRYPTION? WHAT IS IT

Encryption is the process of encoding messages or information in such a way that only authorised parties can read it.

WHY IS IT IMPORTANT

Encryption is important because it allows you to securely protect data you don't want anyone else to have access to.

IT HAS BEEN PROVEN THAT OPTICAL FIBRE IS INHERENTLY INSECURE

MYTH

Optical fibre is inherently secure

TRUTH

Anyone with mischief or criminal intentions can access data anywhere along an optical cable that is not adequately protected

- Low-cost, passive, non-intrusive optical monitoring devices have emerged and are widely available a such as works by bending fibre bending it sufficiently to extract a signal without damaging the fibre or disrupting communications to sender and recipient.
- Even dedicated or dark fibre used by a single company point-to-point is vulnerable



Inexpensive, easily accessible hacker's clip-on coupler device



Tapping Possibilities

¹ FORMER US ARMY GENERAL AND WHITE HOUSE CHIEF OF STAFF, DEMONSTRATED ON "21ST CENTURY BUSINESS" CHANNEL.
SEE [HTTP://WWW.SENETAS-EUROPE.COM/SE_SITE_2011/NW_ENCRYPTION/SENETAS/21ST_CENTURY_BUSINESS_CLIP.HTM](http://www.senetas-europe.com/SE_SITE_2011/NW_ENCRYPTION/SENETAS/21ST_CENTURY_BUSINESS_CLIP.HTM)

2014/15: THE YEAR OF ENCRYPTION



10 January 2014 Last updated at 00:05 GMT

2014: The year of encryption

By Paul Rubens
Technology reporter

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

*Strategic insights and
bipartisan policy solutions*

2014 as the Year of Encryption: A (Very) Brief History of
Encryption Policy



By James Andrew Lewis
JAN 10, 2014

Unisys Security Experts Predict 2014 Will Be “The
Year of Encryption” as Organizations Combat
Growing Cyber Threats

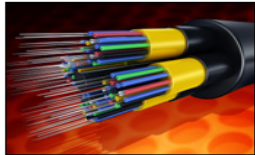
EVERYWHERE YOU LOOK...

CIO TODAY
Daily Briefing for Technology's Top Decision-Makers

Enterprise Software
Enterprise Hardware
Network Security
Cloud Computing
CRM Systems

Did NSA Secretly Tap the Internet Backbone?

By Barry Levine
November 26, 2013 12:55PM



Earlier this month, reports surfaced that the documents released by former NSA contract employee Edward Snowden showed the NSA had tapped the transmissions to and from Google's and Yahoo's data centers. The taps meant that the agency had access to hundreds of millions of user accounts, many of which are owned by Americans.

SHARE

THE WALL STREET JOURNAL. TECH **US\$1 A WEEK**

TECHNOLOGY

Tech Firms Push to Control Web's Pipes

Google, Facebook Raise Tensions With Telecoms in Power Struggle for Internet's Backbone

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION VIDEO

Our Government Has Weaponized the Internet. Here's How They Did It

BY NICHOLAS WEAVER 11.13.13 9:30 AM

Follow @ncweaver

Share 5.1k
Tweet 2,436
g+1 774
in Share 236
Pin it

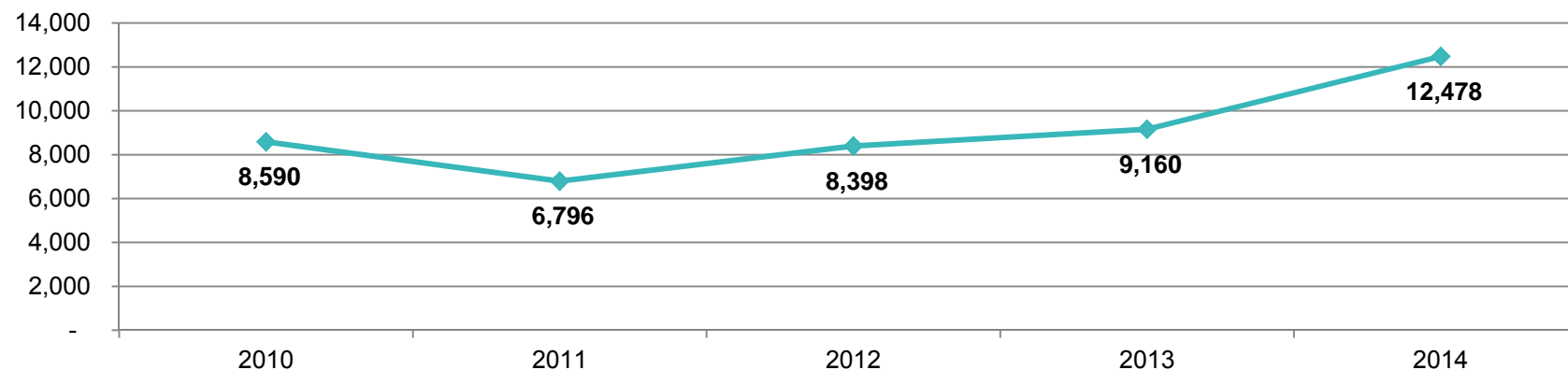
2.0 | FINANCIAL PERFORMANCE & GO TO MARKET MODEL

30 JUNE 2014 RESULTS HIGHLIGHTS

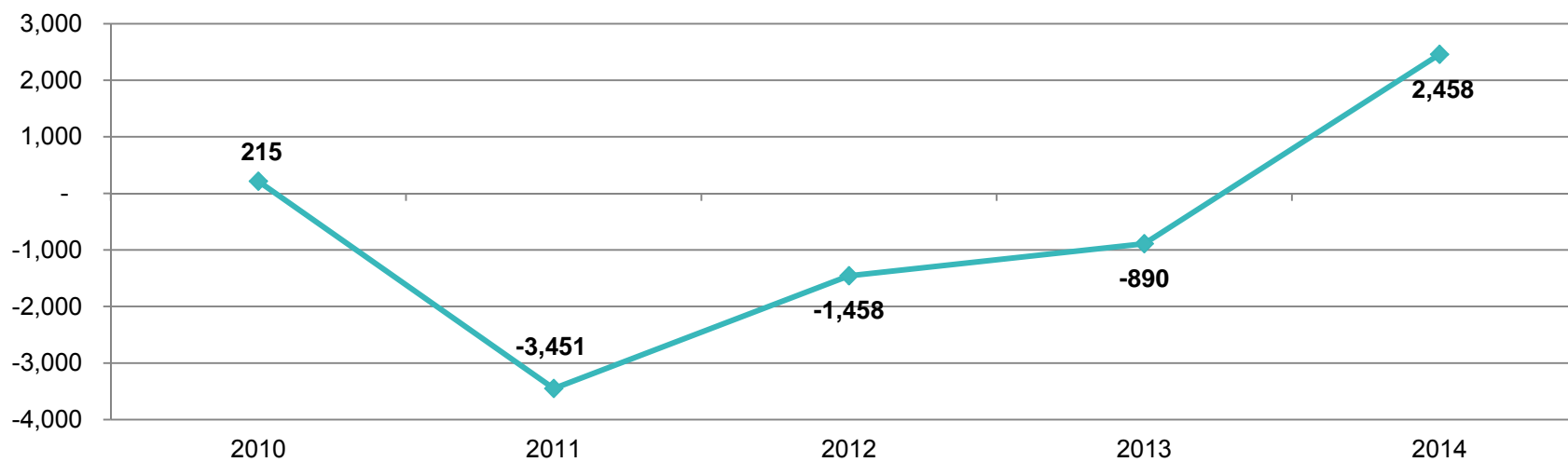
- \$44% increase in operating revenue to \$11m;
 - Increased in international sales from SafeNet
 - Increased maintenance income
- 2014 NPBT of \$2.5m vs 2013 loss before tax of \$893k;
- R&D tax refund of \$1.4m;
- 40% increase in net assets to \$8.5m;
- Debt free and strong improvement in operating cash flows; and
- \$6.8m cash at bank at 30 June 2014, at 14/10/14: \$10m.

HISTORICAL REVENUE & PROFIT PERFORMANCE

Total Revenue \$'000



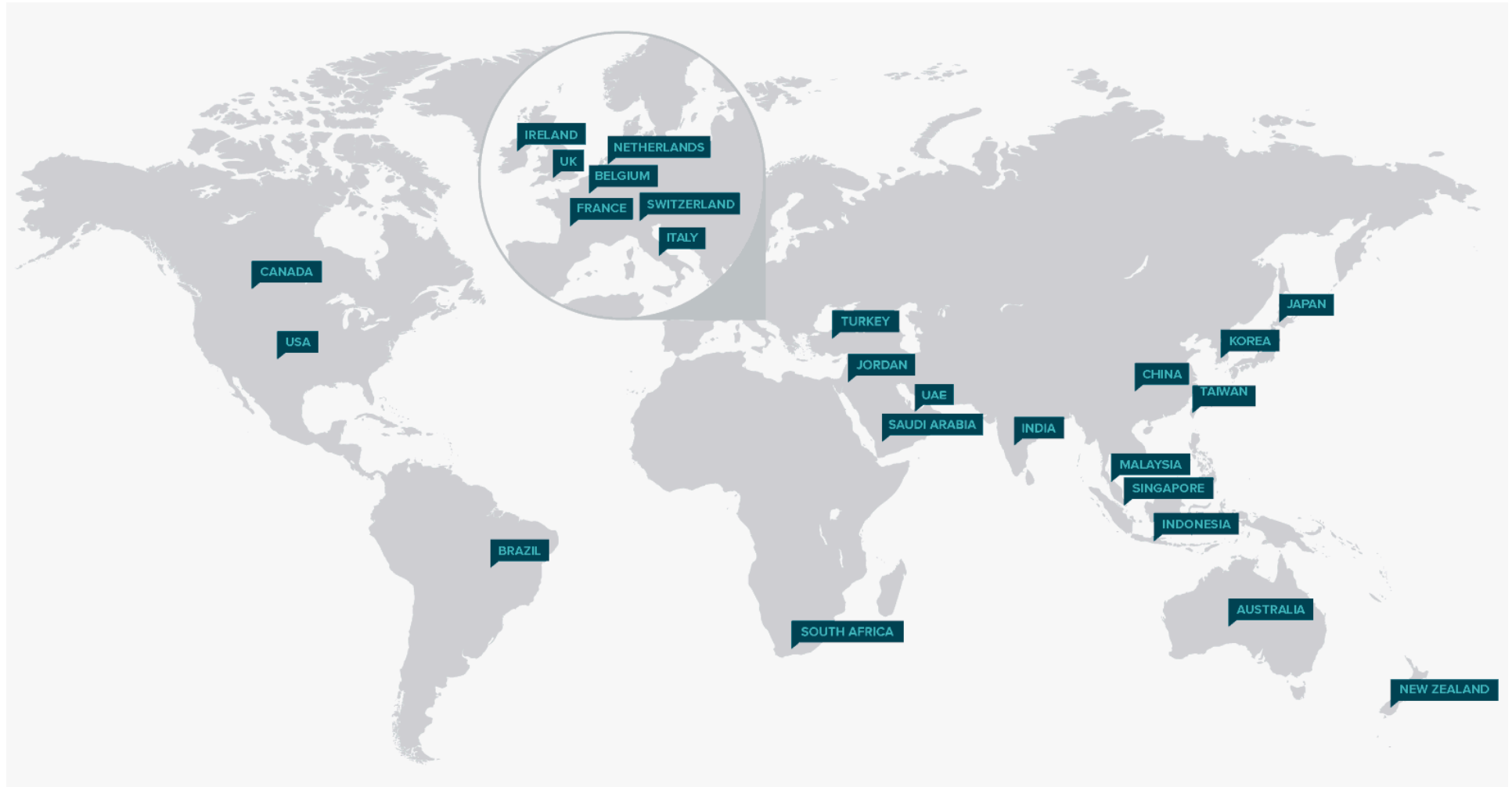
Net Profit Before Tax \$'000



GO TO MARKET MODEL

- Senetas has appointed SafeNet Inc. as its world wide master distributor (excl Australia and New Zealand).
 - SafeNet Inc. reaches across 100 countries and has 25,000 customers; 200+ strong sales force:
 - » Senetas shares in revenue from SafeNet product and maintenance sales;
 - » Senetas manufactures product in Australia on behalf of SafeNet; and
 - » Senetas provides customer support services.
- In Australia and New Zealand, Senetas sells and distributes via a number of partners including SafeNet Inc. UXC Ltd, Nextgen and Hewlett-Packard.

GOVERNMENT, DEFENCE AND COMMERCIAL CUSTOMERS ACROSS 29 COUNTRIES



MARKET DRIVERS

- **GROWING AWARENESS OF RISK TO SENSITIVE DATA**

- Rise in the level of cyber threat;
- Awareness of the risk of vulnerability of data in transit; and
- Growing data volumes = increased use of Layer 2 networks. (in key markets).

- **MATURING REGULATION**

- Data Breach notification and privacy legislation;
- Health Acts including HIPPA in the USA; and
- Financial Prudential Regulation.

- **CHANGES IN TECHNOLOGY**

- Cloud based technologies & data analytics.

ACQUISITION OF SAFENET BY GEMALTO

- 8 August 2014, Gemalto NV ('Gemalto') entered into an agreement to acquire SafeNet;
- Gemalto is a substantial global organisation, with a turnover of US\$3 billion in 2013;
- Senetas should benefit from Gemalto's presence in 45 countries and commercial enterprise sector focus;
- SafeNet's product portfolio (including high-speed encryption supplied by Senetas) is complementary to Gemalto's portfolio and market positioning.

3.0 | TECHNOLOGY

SENETAS ENCRYPTION TECHNOLOGY

- **PURPOSE BUILT ENCRYPTION TECHNOLOGY**
- **OVERCOMES TRADITIONAL ENCRYPTION LIMITATIONS:**
 - Complexity
 - Incompatibility
 - Performance
- **ENCRYPTION PRODUCTS FOR SECURING:**
 - Government & Defence networks
 - Data centres networks
 - Carrier wide area networks
 - Industrial control networks

OUR NEW CN6000 SERIES ENCRYPTORS OF ADVANCED LAYER 2 ENCRYPTION TECHNOLOGY

- Designed to encrypt data at speeds up to 10Gbp/s
- Highly secure, highly resilient wire speed encryption of Ethernet traffic
- More than 2 years R&D with customer input
- Highly certified by 4 independent security authorities

CN4000 10G Ethernet encryptor



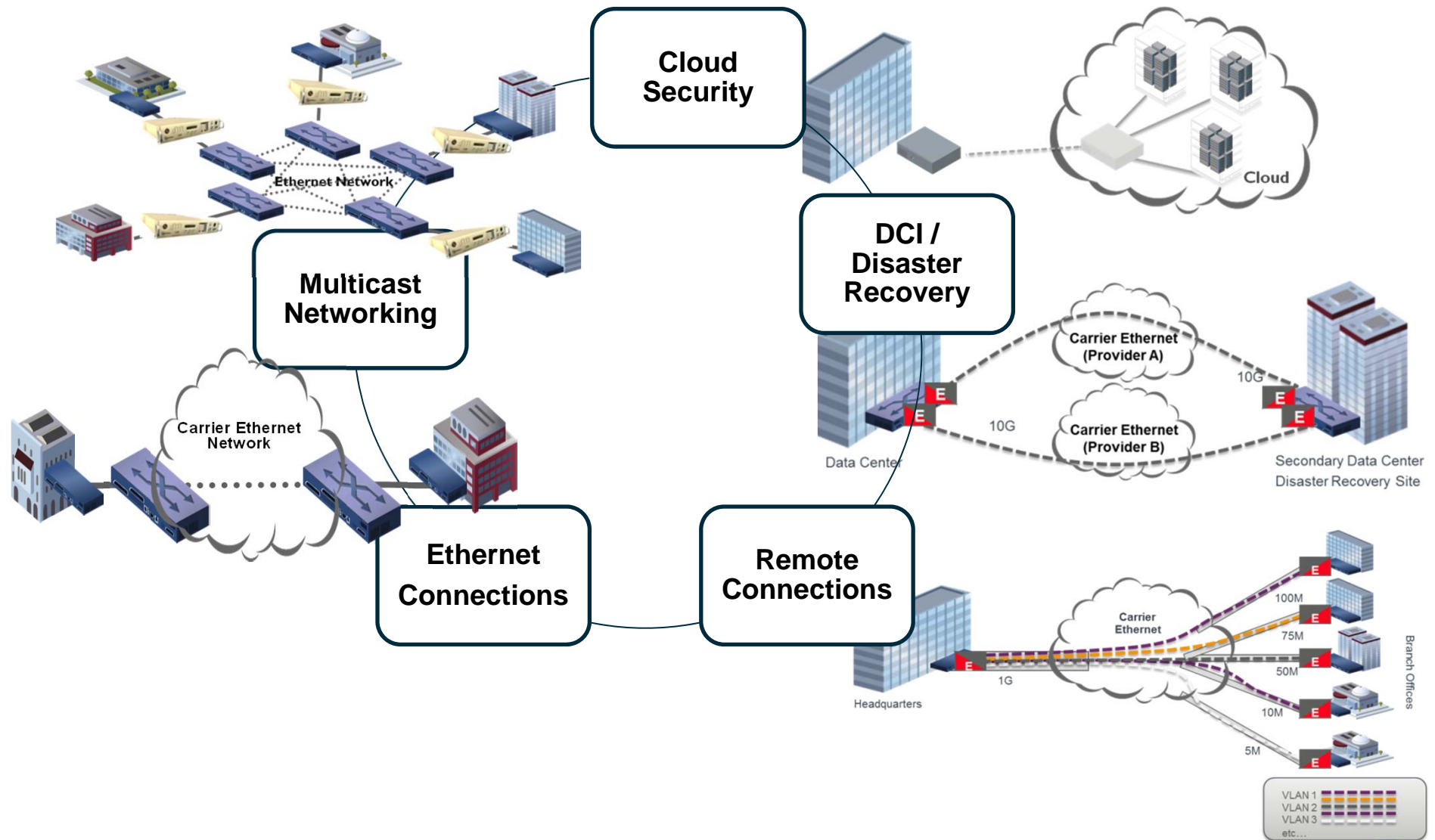
- **Launched March 2014**
- High performance entry level product;
- Designed for SME, Medium enterprises and branch office deployments;
- Small desk-top form factor operating at full line rate encryption up to 1Gbps at Layer 2;
- Fully interoperable with existing CN/CS series of Ethernet devices; and
- Entry-level with full CN Series capabilities.

CN6010 Ethernet encryptor



- **Launched January 2014**
- Expanding the CN6000 series;
- Same enclosure design benefits as incorporated in the CN6100:
 - 1U form factor;
 - Dual hot swappable power supplies; and
 - User replaceable/hot swappable fan tray.
- Fully interoperable with existing CN/CS series of Ethernet devices.

HIGH SPEED IS EVERYWHERE FOR EVERYONE



TRIPLE CERTIFIED SENETAS ENCRYPTION PRODUCTS

Government and Defence

			
<ul style="list-style-type: none">▪ Certification received in March 2012 (certificate numbers 1267 and 1268)▪ Required for purchase of cryptographic products by US Federal Government and defence customers▪ FIPS certification is not the same as “FIPS compliant” or statements like “implements FIPS approved algorithms”	<ul style="list-style-type: none">▪ First certification received in November 2009 (certificate number 2011/77)▪ CC is an international standard (ISO/IEC 15408) for computer security certification▪ CC Evaluation Assurance Level 4 (EAL4 and 2+) is required for Australia and New Zealand customers as well as other foreign governments▪ CC is a collaboration among Canada, France, Germany, the Netherlands, the UK and the US & other countries	<ul style="list-style-type: none">▪ Certification received in November 2012 (certificate numbers 1223355849AES)▪ Required for purchase of cryptographic products by the UK Government and Defence Departments▪ Senetas has the only Layer 2 Ethernet encryptor device available to the UK government and Defence Department to purchase	<ul style="list-style-type: none">▪ Certification received in October 2014 (Certificate Number – N/A)▪ Required for purchase of cryptographic products by the NATO civil and military bodies▪ Senetas has the only Layer 2 Ethernet encryptor device that has completed the certification

RESEARCH & DEVELOPMENT

2014 ACHIEVEMENTS

- **NEW AND INNOVATIVE PRODUCT ENHANCEMENTS**
 - CN4010 entry level encryptor – Now launched
 - CN6010 cost reduced 1 Gb – Now launched
 - CN8000 multi-slot – Trialling with Customers

2015 PROJECTS

- **SPECIFIC MARKET ENCRYPTORS:**
 - Custom algorithm encryptors
- **100G DEVELOPMENT WELL ADVANCED. ESTIMATED RELEASE 2016.**
- **CONTINUING FOCUS ON PRODUCT CERTIFICATIONS (FIPS, CC, UK CPA & NATO).**
- **EXCITING PROSPECTS WITH TECHNOLOGY VENDORS SPECIALISING IN LAYER 2 NETWORKING AND CCTV TECHNOLOGIES.**

4.0 | SUMMARY

NEAR TERM MARKET DRIVERS

- **GROWING AWARENESS OF RISK TO SENSITIVE DATA**
 - Unprecedented level of cyber threat;
 - Awareness of the risk of vulnerability of high speed data transmissions; and
 - Growing data volumes leading to increase in use of Layer 2 networks.
- **NEW DISTRIBUTION DISTRIBUTION RELATIONSHIP WITH SAFENET**
 - Far greater access to key global markets;
 - Direct customer contact with largest customers; and
 - Relationship strongest it has ever been.
- **SPECIFIC MARKET ENCRYPTORS**
 - Custom algorithm encryptors;
 - New NATO certification;
 - Products just released; and
 - New Technology relationship with Layer 2 Network and CCTV companies.

KEY STRATEGIC GROWTH OBJECTIVES FOR 2015

- Continue to deliver strong financial results;
- Grow international sales and extend collaboration with SafeNet in marketing and sales planning;
- Increase focus on Asia, Eastern Europe, Middle East and the commercial market as an opportunity for sales growth;
- Strong commitment to Research and Development;
- Introduction of new products and features;
- Maintain and enhance international security certifications; and
- Focus on new technology relationships with Layer 2 and CCTV technology companies.

| THANK YOU