

19 November 2015

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

Dear Sir/Madam

**SENETAS CORPORATION – 2015 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, 52 Queens Road, Melbourne on Thursday, 19 November 2015 at 10:30 am (Melbourne time).

Yours sincerely



Brendan Case  
**Company Secretary**



SENETAS CORPORATION LTD  
AGM 19 NOVEMBER 2015  
CHAIRMAN'S OPENING ADDRESS

I would like to welcome you today to the annual general meeting of Senetas Corporation Ltd and thank you for the interest demonstrated by your attendance today.

Let me start by welcoming our Board. On my left is our CEO Andrew Wilson. Next to Andrew is Lachie Given, on Lachie's left is Dave Hansen who has recently joined our board, and on the far left is Lt Gen Ken Gillespie.

I welcome Dave to his first Senetas AGM and thank all the board for their tireless input over the past 12 months. They are available at any time to assist your company's growth and their input has been critical to your company's success. I would also like to thank our staff who have put in a fabulous effort over the past 12 months and especially the senior management team. Julian Fay - CTO, John Weston - Chief Engineer, Barb McMeekin - CFO and Simon Galbally - marketing director.

Last Saturday morning, we awoke to the horrible news of multiple terrorist attacks in the heart of Paris, France which left over 120 people dead and hundreds wounded. We feel especially affected by these tragic circumstances as our global distribution partner Gemalto is headquartered in Paris. Our hearts and prayers go out to all who work at Gemalto, their families and friends. On behalf of Senetas I would like to express our solidarity with the people of France and all who have been affected by these truly horrific and tragic events.

These events did give me cause to reflect on the uncertain and dangerous times in which we live - and the need to be aware of our own personal security. Absolute physical security is impossible to achieve. For us to go about our daily lives there is an element of risk we have to accept. But there are many things we do not do because common sense tells us the risk we are assuming is too great.

Similarly in the digital or cyber world, total security in the sense of full protection from data thieves is not possible. Data thieves will always manage to find network vulnerabilities which they will exploit, and this is



why robust encryption technologies are so important in order to guarantee that stolen data is useless in the hands of the thieves and other unauthorised access.

What amazes me is that those who should know this fact - CIO's CEO's, CFO's, Presidents, Vice Presidents, managing directors and boards of directors of large organisations, government and non-government - still do little or nothing to ensure that the data held by the organisations they lead cannot be used by anyone if for some reason it were unlawfully accessed. We constantly read of data network breaches such as theft of credit card information and the losses associated with these breaches was US\$8 Billion in 2014.

Two recently publicised data thefts have again highlighted the complacency of the leaders of major government and non-government organisations when it comes to protecting sensitive data. In one case the failure to protect data has led to a congressional hearing in the United States and the resignation of the head of the US Office of Personnel Management. In this case over 20 million records of US Government personnel were unlawfully accessed via unprotected networks and other security weaknesses. While allegedly breached by Chinese hackers, these US federal government employees had all their identity and personnel record information stolen. What they stole also included documents used for conducting background checks for worker security clearances. These documents contain a wealth of sensitive information about employees' identities, backgrounds, their friends and family.

The second incident occurred at home here in Australia. As far as I am aware there have been no repercussions over this incident - the accessing of the Australian Government's secret submarine plans. But there certainly should be. Too often those charged with protecting data take the easy option of doing nothing and hoping that nothing will happen. This behaviour is referred to as apathy and 'tick-the-box' mentality, although it may be better described as negligence.

At Senetas we see this happen repeatedly at the highest levels of government and non-government organisations which hold very sensitive data. Further, the incidence of reported data theft is much lower than the actual occurrences of data theft and is often reported well after the event.



When we think about security, there is quite properly, a concentration on physical security and this will likely be more so since the Paris bombings. However, the Australian government must focus on cyber-security as a national security priority issue. Cyber-security is part of an overall security strategy. One needs to prevent identity theft and also the risk of a cyber terrorist attack on critical infrastructure. The only way to do this is to ensure that sensitive data is robustly encrypted.

Furthermore, an effective national data security strategy is essential to Australia's digital economy. And just like our well regulated corporations sector and other like initiatives that add strength to the world view of our economy; a strong national security strategy will help differentiate the Australian economy as a safe place to invest. Such a security strategy demands the implementation of data breach notification laws and direct sanctions against executives and boards that do not protect the sensitive data they control. I am very encouraged that our Prime Minister, Malcolm Turnbull, understands that a cyber security strategy is not just about ticking boxes. He has just recently rejected the draft Government cyber security strategy report as it lacked teeth and funding.

Senetas had an excellent 2015 financial year and I thank Andrew Wilson for his leadership during the year. Andrew will take you through the detail. I would like to make the following comments on our strategy and plans for continued growth, improvement and maintaining our position as the world's leading layer 2 high speed encryption developer.

Senetas is a growth company. We have built strong cash reserves to cushion us from unforeseen external shocks, enable us to reinvest in developing new products for the marketplace and make acquisitions where appropriate. We will be demonstrating our 100Gbps product to customers early next year.

We are also well advanced on our custom encryptor product for a major European customer and in developing a virtual encryptor for software defined network environments. And we have made many additional improvements to our existing product-set to meet new and emerging customer needs. We expect these initiatives will drive revenue and profit growth for FY17 and beyond.



But we need to think even further ahead for what the market will require. What does 2018 and beyond look like? Where are there gaps in the market? Can we fill them?

We are planning for these now. It is partly for these reasons that I asked Dave Hansen to join our board. His vast IT and security sector experience and his current work in private equity will help us in our planning.

Senetas is also establishing an advisory board with additional outside expertise to assist us in our planning. Finally we work very closely with the Gemalto team in guiding and directing our market and customer-focused engineering efforts.

This investment in planning and engineering will ensure that we will achieve sustainable continued strong revenue and profit growth in the years to come.



# **SENETAS CORPORATION LIMITED**

## **ANNUAL GENERAL MEETING 2015**

# **CHAIRMAN'S ADDRESS**

## **MR FRANCIS GALBALLY**



# THE AUSTRALIAN

WWW.THEAUSTRALIAN.COM.AU | THE HEART OF THE NATION



\$2.70  
MONDAY  
November 9, 2015  
1100-1200 PM  
1200-1200 PM

**WIN**

**10-NIGHT LUXURY KIMBERLEY CRUISE**

**\$50,000 IN PRIZES**

DETAILS P13

**SCORE A \$500 RM WILLIAMS GIFT CARD EVERY DAY**

**MEDIA**

**GOODBYE GYNGELL**

Nine chief hands over the controls (P23) + Sharri Markson's must-read Media Diary (P24)



REVEALED 'TOP SECRET' DETAILS HAND-DELIVERED AS FOREIGN SUBMARINE BIDDERS REPORT CYBER ATTACKS

## China, Russia hack sub plans

CAMERON STEWART

Chinese and Russian spies have attempted to hack into the top secret details of Australia's future submarines, with both Beijing and Moscow believed to have mounted repeated cyberattacks in recent months.

The hacking attempts have been aimed at the submarine builders in Germany, France and Japan bidding for the \$20 billion contract to build the new fleet. The

bidders are holding highly sensitive information about the Royal Australian Navy's technical requirements for its new generation submarines.

The hacking attacks have forced the bidders to rely more heavily on hand-deliveries of the most sensitive information. And they are understood to have alarmed the federal government, which has raised the issue of cyber security with each of the three foreign bidders for the submarine contract. German shipbuilder

ThyssenKrupp, France's DCNS and the Japanese government.

Manfred Klein, campaign manager Australia for Germany's TKMS, said at the company's submarine shipyard in the German port of Kiel: "We have about 30 to 40 [hacking] attempts per night. That's what our IT people say."

Mr Klein said the cyberattacks were all directed at the submarine facility in Kiel and came at a time when the shipyard had a team of 120 people finalising its design for the future Australian submarine.

"The Australian government has raised it with us, and they think it's significant," said TKMS Australia board member Jim Duncan, who is helping put together the German bid.

TKMS Australia chairman John White said the attempted industrial espionage was to be expected on such a sensitive and important defence project. "They're trying to get into everyone's communications," Dr White said. "Espionage and breaches of security... you just assume it is

happening. Everybody is in that game. It's a space that people play in. We don't suspect anyone, we suspect everybody."

The Australian understands Japan and France are concerned about attempts by suspected foreign powers to hack into information relating to the sub project.

TKMS declined to say which countries were behind the attempted hackings, but all three foreign bidders privately believe China is leading the push to glean information about the submarine

project. Other strategic rivals including Russia are also suspected of recent hacking attempts and it is also possible the three bidders for the lucrative contract are seeking to spy on each other.

There is no evidence to suggest that any classified information has so far been compromised by the attempted hacks, which are thought to be from state-run intelligence agencies, commercial companies and individuals.

The espionage comes at a time of growing strategic naval com-

petition in the Asia-Pacific, with China ramping up its submarine building program and asserting its territorial claims on disputed islands in the South China Sea. Russia has also stepped up naval activities in the region, while other Southeast Asian nations are seeking to modernise their submarine capabilities.

As part of the competitive evaluation process for the future

Continued on page 5

COMMENTARY P10

## PM's bid to unlock Kerr's letters

EXCLUSIVE

PAUL KELLY  
TROY BRAMSTON

Malcolm Turnbull plans to advise the Governor General and the Queen to release correspondence between former governor general John Kerr and the palace leading to the dismissal of the Whitlam government.





Big Obama Donors Stay on Sidelines in 2016 Race



Not Guilty Verdicts on All Counts in 'Goodfellas' Case



Border Agents Get Body Cameras



Tolerance, Free Speech Collide on Campus



Miss Denies B Student Making




U.S.

## U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say

Described as one of the largest thefts of government data ever seen

By [DEVLIN BARRETT](#), [DANNY YADRON](#) and [DAMIAN PALETTA](#)

 572 COMMENTS

Updated June 5, 2015 6:33 a.m. ET

U.S. officials suspect that hackers in China stole the personal records of as many as four million people in one of the most far-reaching breaches of government computers.

The Federal Bureau of Investigation is probing the breach, detected in April at the Office of Personnel Management. The agency essentially functions as the federal government's human resources department, managing background checks, pension payments and job training across dozens of federal agencies.

### Most Popular Videos

1. iPad Pro Video Review



2. Rubber Ducky Puts Bluetooth in the Bath



3. Kurds Launch Offensive to Retake





ADVERTISEMENT

Technology | Mon Oct 19, 2015 8:39pm EDT

Related: TECH

# China tried to hack U.S. firms even after cyber pact: CrowdStrike

BY JOSEPH MENN



A man types on a computer keyboard in Warsaw in this February 28, 2013 illustration file picture.  
REUTERS/KACPER PEMPEL/FILES

Hackers associated with the Chinese government have tried to penetrate at least seven U.S. companies in the three weeks since Washington and Beijing agreed not to spy on each other for commercial reasons, according to a prominent U.S. security firm.

CrowdStrike Inc said software it placed at five U.S. technology and two pharmaceutical companies had detected and rebuffed the attacks, which began on Sept. 26.

## PHOTOS OF THE DAY



Our top photos from the last 24 hours. [Slideshow »](#)

[Battling Islamic State](#)

[Shore of dreams and nightmares](#)

[Hong Kong's McSleepers](#)

ADVERTISEMENT

## TRENDING ON REUTERS

U.S. bombers flew near China-built island in South China Sea: Pentagon 1

IS video threatens attacks in Russia 2

Two suicide bombers hit Hezbollah bastion in Lebanon, 43 killed | VIDEO 3

China

# Chinese hack of US national security details revealed days after Russian hack

Government sources tell NBC News that Chinese attack targeted personal emails of 'all top national security' officials just days after Pentagon hack

Sam Thielman in New York

@samthielman

Tuesday 11 August 2015 05.33 AEST

Comments

120

Save for later



A reported spear-phishing attack on the Pentagon's Joint Staff email system exposed some 4,000 civilian and military employees and is believed to have been sponsored by Russia. Photograph: AFP/Getty Images

The ongoing saga of successful foreign hack attacks on government databases continued Monday with news of another break-in allegedly perpetrated by [China](#).

## Most popular in Australia



Collapsing Greenland glacier could raise sea levels by half a metre, say scientists



America's poorest white town: abandoned by coal, swallowed by drugs



Agency behind #YourTaxis campaign fired after social media disaster



Apple apologises after saying black students 'might steal something'





# AGENDA

- FY15 financial highlights
- Sustainable platform for the future
- Investing for continued growth
- Key growth drivers
- Summary and outlook

# FY15 HIGHLIGHTS

## Strong financial position

- Operating revenue increased 47% to \$16.2m: Net profit before tax up by 145% to \$6.0m.
- Strong balance sheet and cash flows.

## Sustainable platform for the future

- Strengthening relationships with major global partners and customers.
- Positive sector thematics:
  - Massive growth in global data usage for the foreseeable future.
  - Continually increasing focus on both data security and network efficiency.
  - Increasing cyber security threat levels.
- Investing in new product development and partner / customer relationships to drive future growth.

# FY15 FINANCIAL OVERVIEW

	FY15 \$000's	FY14 \$000's	Change
<b>Revenue from ordinary activities</b>	16,207	11,038	47%
<b>Profit before tax</b>	6,021	2,458	145%
<b>Net profit after tax</b>	4,016	2,957	36%

Operating revenue increase of \$5.2m:

- 41% growth in product sales.
- 55% increase in maintenance revenue.
- Growth in revenue driven primarily by orders from new customers and increasing maintenance revenues.

Gross profit was \$13.4m; a gross margin of 83%.

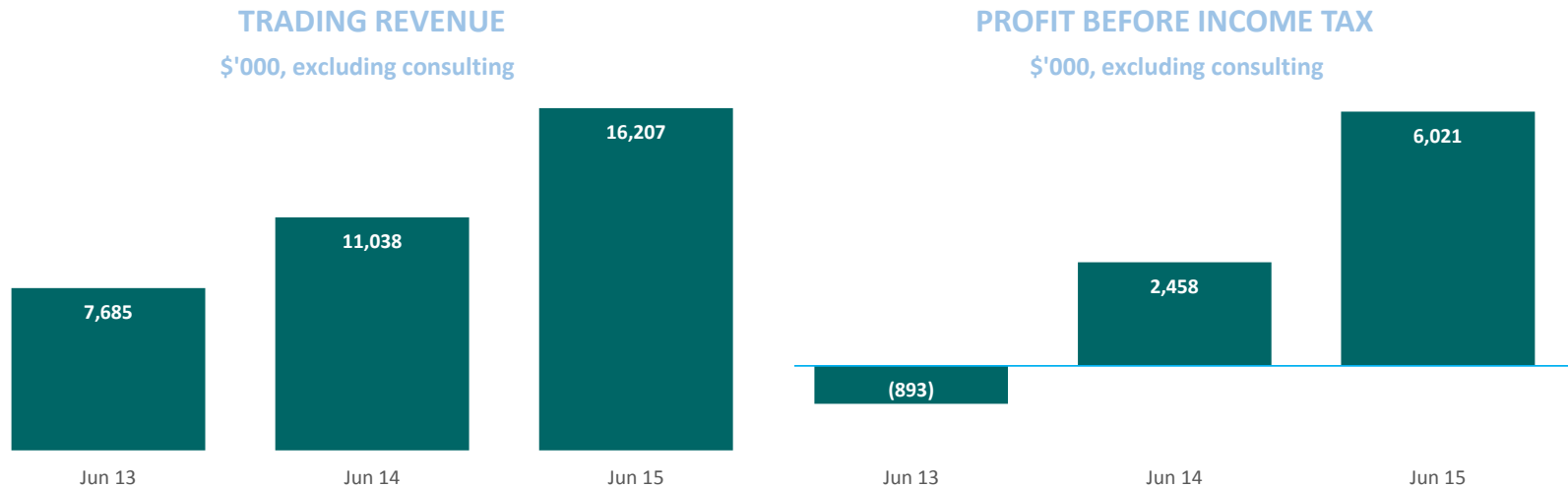
Operating expenses were \$9.1m vs \$8.3m in FY14.

Net profit before tax increased by 145% to \$6.0m & net profit after tax rose by \$1.1m:

- Tax expense of \$2.0m in FY15 (benefit of \$0.5m in FY14).



# SUSTAINABLE GROWTH



## Revenue growing

- 44% revenue growth in FY14 followed by 41% revenue growth in FY15. Maintenance is now 36% of operating revenue 34% in FY14.
- Strong sales results from Gemalto in December 2014 & June 2015.

## Growth track record

- FY15 was the first full year of benefit from the improved agreement with SafeNet / Gemalto.
- Driven by leveraging the master distributor relationship, improved sales planning and execution and strong cost control.

# STRONG OPERATING CASH FLOWS

	FY15 \$000's	FY14 \$000's	Change
<b>Operating cash flows</b>	9,577	2,879	233%
<b>R&amp;D tax concession</b>	1,386	1,359	2%
<b>Investing cash flows</b>	(470)	(110)	4x

Strong growth in operating cash flows.

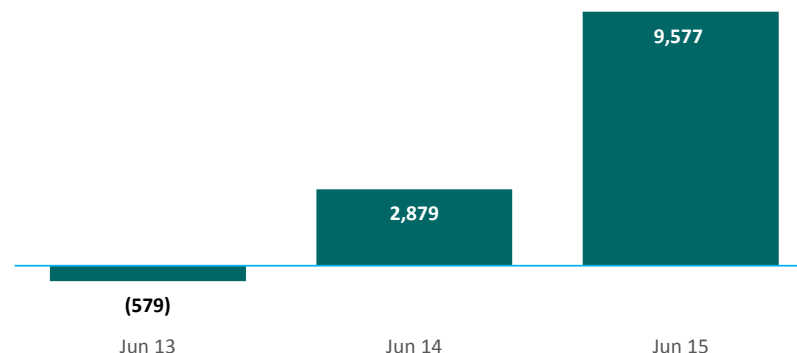
- Continued discipline with costs while growing core revenue.

Cash balance of \$15.9m at 30 June 2015

- Flexibility for disciplined investment in organic and acquisition opportunities in the future.
- Reflects rapid return to profitability and strong cash flow conversion.

## NET CASH FLOW FROM OPERATIONS

\$'000



# SHARE PRICE PERFORMANCE



# INVESTMENT FOR CONTINUED GROWTH



# INVESTING IN THE BUSINESS

## Building capability to drive medium term growth

- Accelerate R&D roadmap and launch projects to maintain market leading position.
- Virtualisation of encryption – developing technologies in response to changing networking protocols and ways of managing networking.
- Custom algorithm offerings – including non US Elliptic Curves.

R&D investment is expected to be higher than normal in FY16 (approx. 30% increase over FY15) – driving revenue growth in FY17 and beyond

- Increased certification costs for planned new product releases.
- Additional engineers and technical support staff.
- Increased non-recurring contractor costs.

# INVESTING IN THE BUSINESS

## International sales support

- Additional Senetas staff in critical markets to assist Gemalto sales teams, guide strategic accounts and projects.
- Building sales focus with our key partners.

## Increasing investment in technology partners and end customers to drive revenue growth opportunities

- Developing new technology relationships with organisations like Avaya (Multinational Networking Vendor).
- Investing in product enhancements to provide more seamless customer experiences across devices and networks.
- Fostering direct strategic end customer relationships.

# GROWTH DRIVERS AND OUTLOOK





# 5 KEY GROWTH DRIVERS

1. Accelerate growth in key high speed encryptor (HSE) markets in partnership with Gemalto to leverage their increased sales and marketing footprint.
2. Develop new opportunities in low HSE penetration including markets such as India, Japan, Singapore, South America, Eastern Europe, France, Germany and Italy by working closely with Gemalto.
3. New faster and 'high-density' products – market-leading encryptors that reflect emerging customer security needs – faster 100Gbps and 'high-density' (multi-port) platforms.
4. New custom algorithm projects leveraging Senetas' unique electronics engineering capabilities and products – custom software toolkit to address unique requirements for other customers.
5. New technology partnerships to expand the reach and capabilities of Senetas products e.g. – an agreement signed with Avaya in January 2015 will provide access to Avaya 'Fabric Connect' network technology and its large customer base around the world.

# SUMMARY AND OUTLOOK

- Senetas is building a strong track record of sustainable profit growth and cash flow.
- Robust balance sheet to support disciplined investment in organic and potential inorganic growth initiatives in the future.
- Strong pipeline of new products built to meet the needs of our most important customers.
- Strong industry fundamentals and increased focus on driving sales execution in partnership with our key partners is expected to deliver profit and cash flow growth in FY16.
- With the benefits of the new master distributor agreement now fully realised and an increase in R&D investment rates over the next 12 months, we expect that profit growth may moderate from that achieved in FY15.
- Medium term profit growth is expected to remain strong as new products are released into the market.



# **SENETAS CORPORATION LIMITED**

## **ANNUAL GENERAL MEETING 2015**