

Cyber security: European emerging market leaders / January 2017
Security: a board-level issue for organisations ^{p4} / The industry is responding ^{p8} /
Emerging market leaders ^{p10}

Cyber security: European emerging market leaders

“There are two types of companies: those that have been hacked, and those who don’t know they have been hacked.”

John Chambers, ex-CEO of Cisco

The total number of security incidents detected by respondents climbed to **42.8 million in 2015**, an increase of 48% over 2013, according to the latest edition of our annual Global State of Information Security survey. That is the equivalent of **117,339 attacks every day**. And the growing significance of cyber security in today's world looks only set to continue as both the number of connected devices and the data that these devices generate continues to increase.

As solutions become increasingly complex, the cyber security industry is responding. Service providers who are able to complement vendor's 'off-the-shelf' products with proprietary and/or bespoke solutions are taking the lead. In particular, **specialist security service providers, with managed security service (MSS) capability and cross-border footprints, appear best-positioned** to address customers' fast evolving needs.

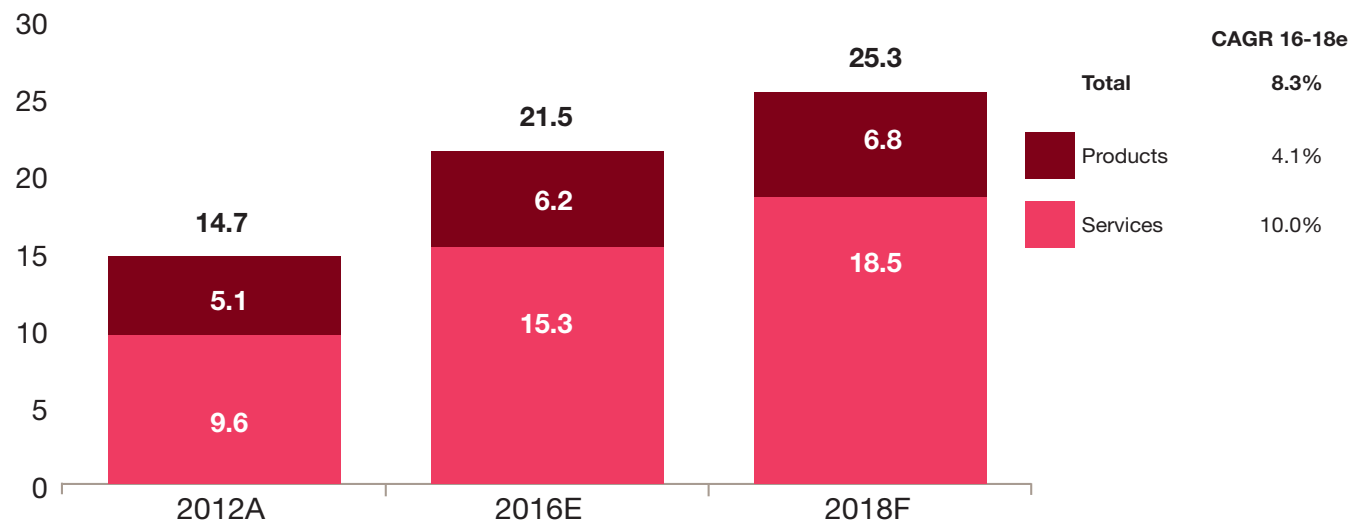
Security: a board-level issue for organisations

Over 90% of the world's data has been generated in the last 5 years¹. Corporations and government agencies globally are increasingly focused on threats of hacking and data theft, and stepping up to safeguard their intellectual property, customer and financial information.

The cost of cyber security breaches can be significant. A leading US retailer declared costs of c.\$162m after hackers stole personal records and credit card details of more than 40m customers in 2013. These costs exclude reputational, fines and legal damages.

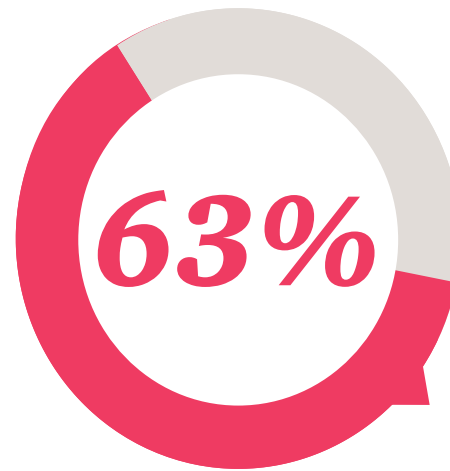
The **European cyber security market** of products and services protecting organisations from such breaches was worth **\$22bn in 2016 and is expected to grow at 8% p.a. to 2018**, predominantly driven by **increasing spend on services**.

Cyber security spending, Western Europe, \$bn, 2012-2018F



Note: Forecast in constant 2014 \$
Source: Gartner, PwC

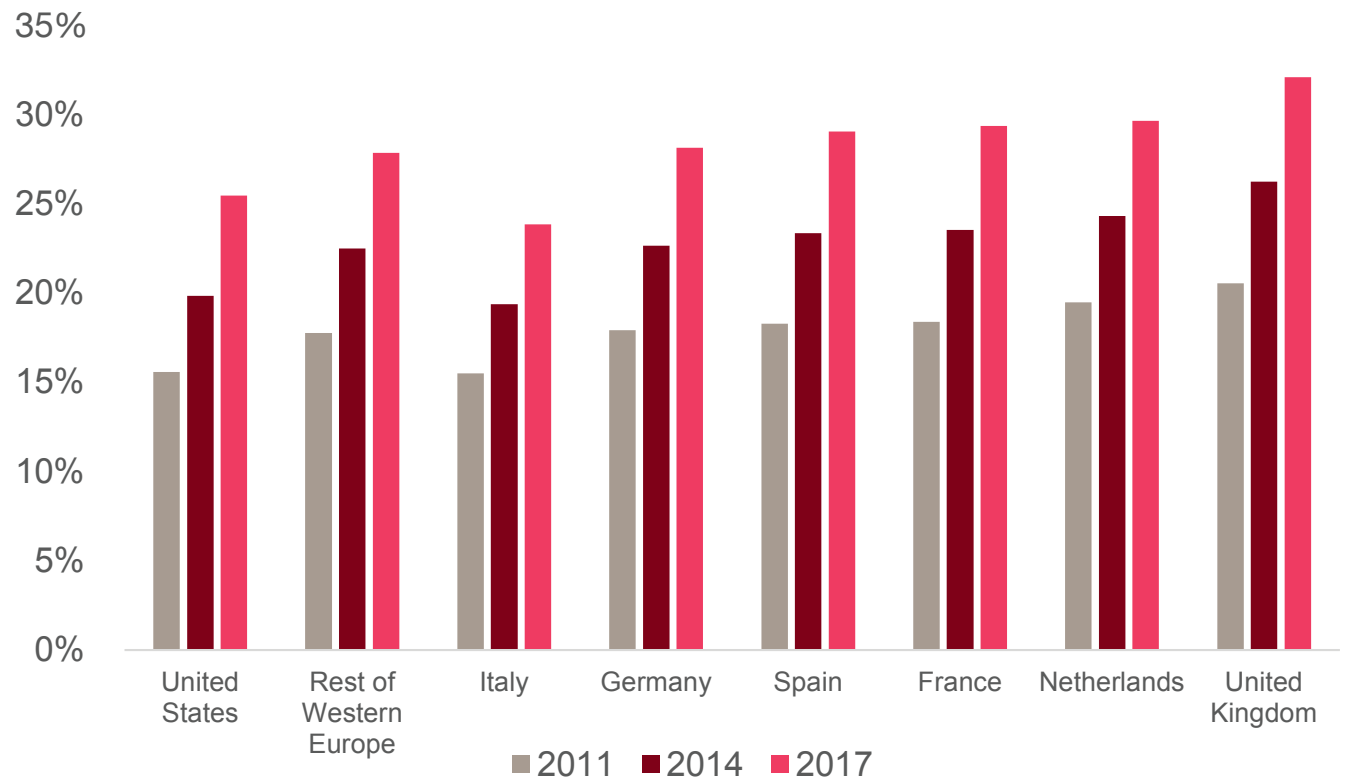
¹ Åse Dragland, SINTEF, May 2013



Organisations' IT footprints have become increasingly complex, driving demand for **more sophisticated and bespoke solutions**. A growing proportion of organisations (often lacking the required expertise in-house) are also deciding to **outsource their cyber security entirely, procuring managed security services (MSS)**.

Managed security services (MSS) are security services either outsourced to a service provider or via a specialist in-house team that oversees cyber security, e.g. round-the-clock monitoring, management of intrusion detection systems and firewalls, performing security assessments, antivirus and anti-spam scanning, etc.

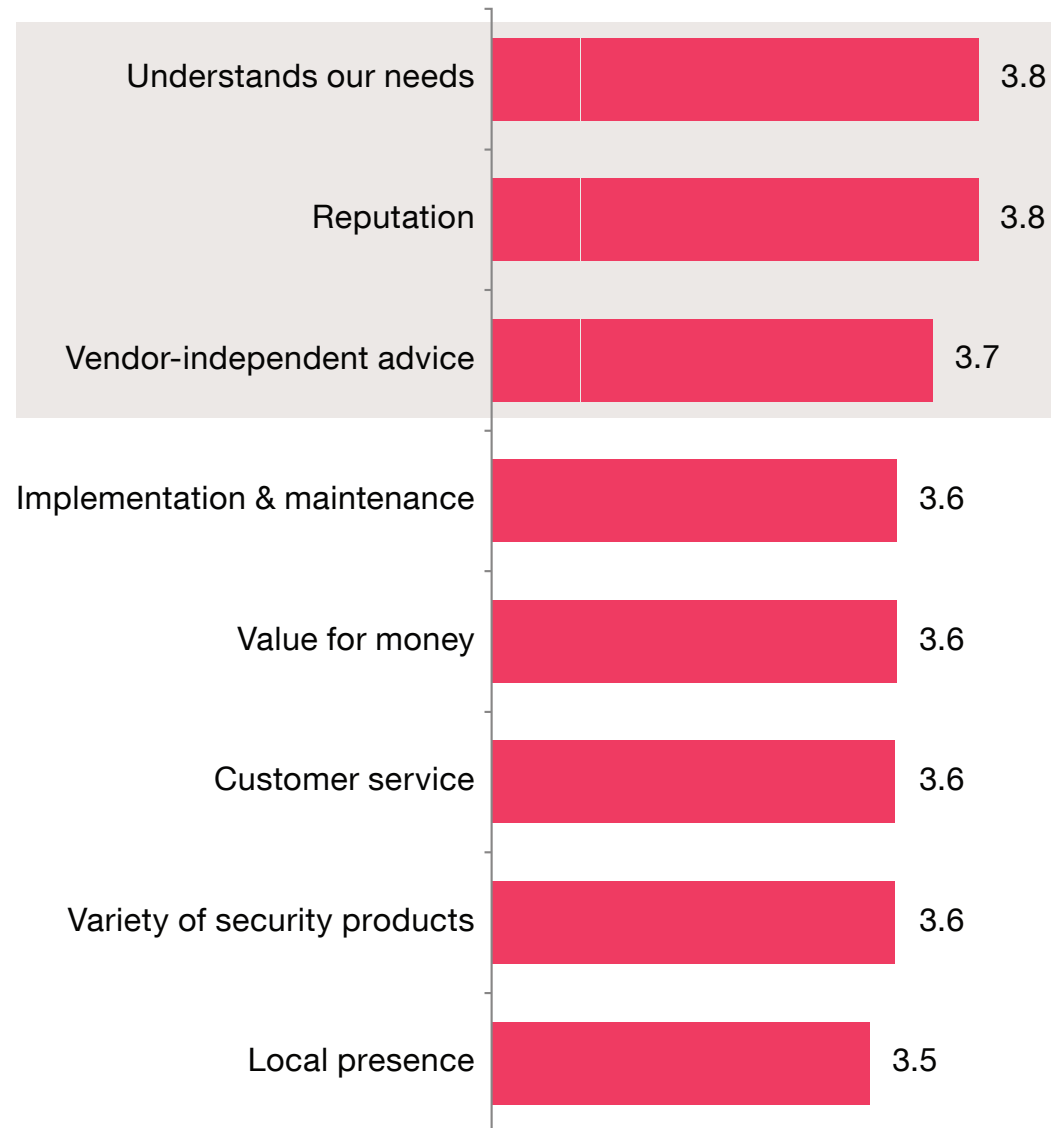
Cyber security outsourcing as a % of total Cyber security spend



Source: Gartner IDC, PwC analysis

As organisations look to outsource their cyber security, they are looking for service providers that understand their security needs, have a proven track record and established market reputation, and are able to provide vendor-independent advice.

Key purchase criteria when selecting cyber security providers

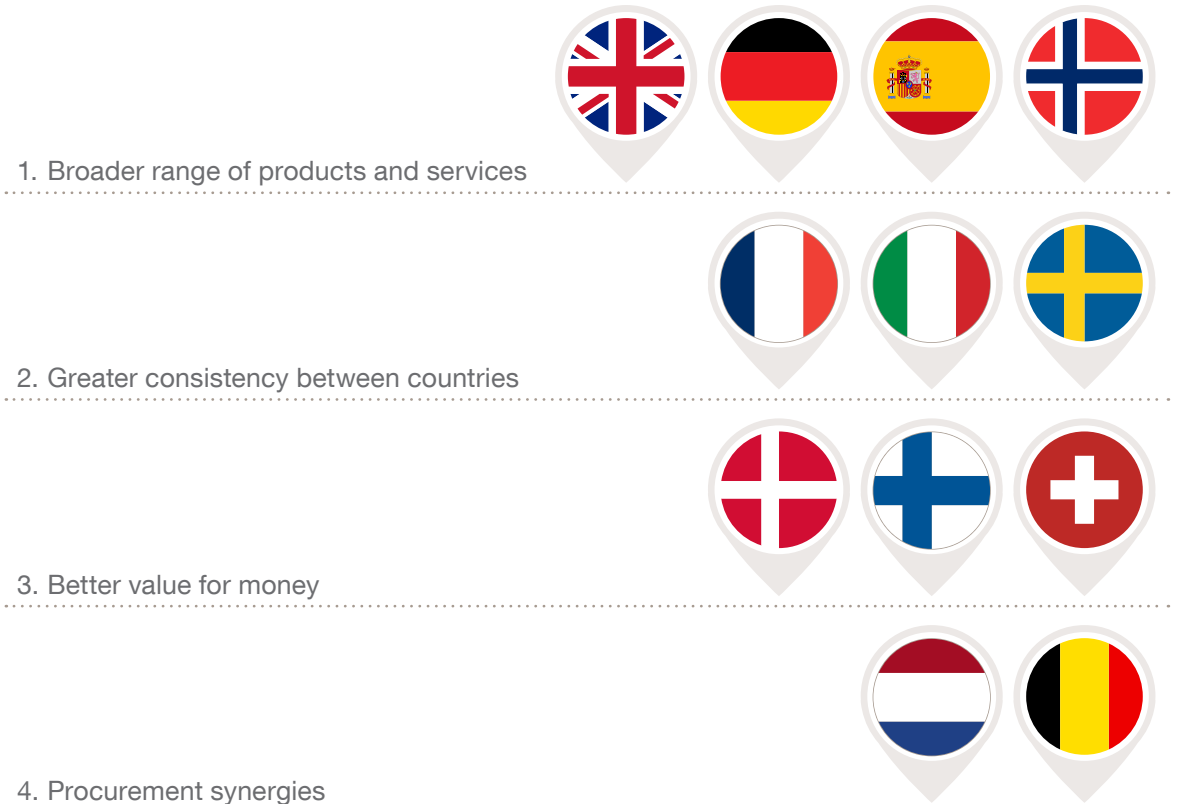


Source: PwC cyber security buyer survey

There is also growing demand for pan-European providers who have the breadth and depth of security expertise and are able to deploy and manage this in a consistent manner across geographies².

Drivers of demand for pan-European providers

#1 reason for choosing to work with pan-European Cyber security solution providers rather than national, by country



Source: PwC cyber security buyer survey

² PwC survey of cyber security buyers, Western Europe, Nov 2015, n=1,275

The industry is responding

There are a number of types of service provider addressing the cyber security needs of businesses today. Amongst Telecom operators, System Integrators (SIs), generalist Value Added Resellers (VARs) and cyber security specialist VARs, there are very differing degrees of focus and competency in cyber security provision, as well as differences in the size of businesses served. Today, **specialist cyber security VARs** distinguish themselves with a unique market positioning, typically serving the **cyber security product resale and implementation needs of small and medium sized businesses.**

Service provider types and typical characteristics

Service provider type	Customer segment served	Cyber security focus	Competencies				
			Product	Networks	Implementation	Managed/outsourcing services	Hosting
Telco	Enterprise & SME		(✓)	✓	(✓)		
SI	Enterprise			✓	✓	✓	(✓)
Generalist VAR	SME		✓	(✓)	(✓)		(✓)
Security focussed VAR	SME	✓	✓	(✓)	✓		

Key

✓ Core competency

(✓) Secondary competency

Source: PwC analysis

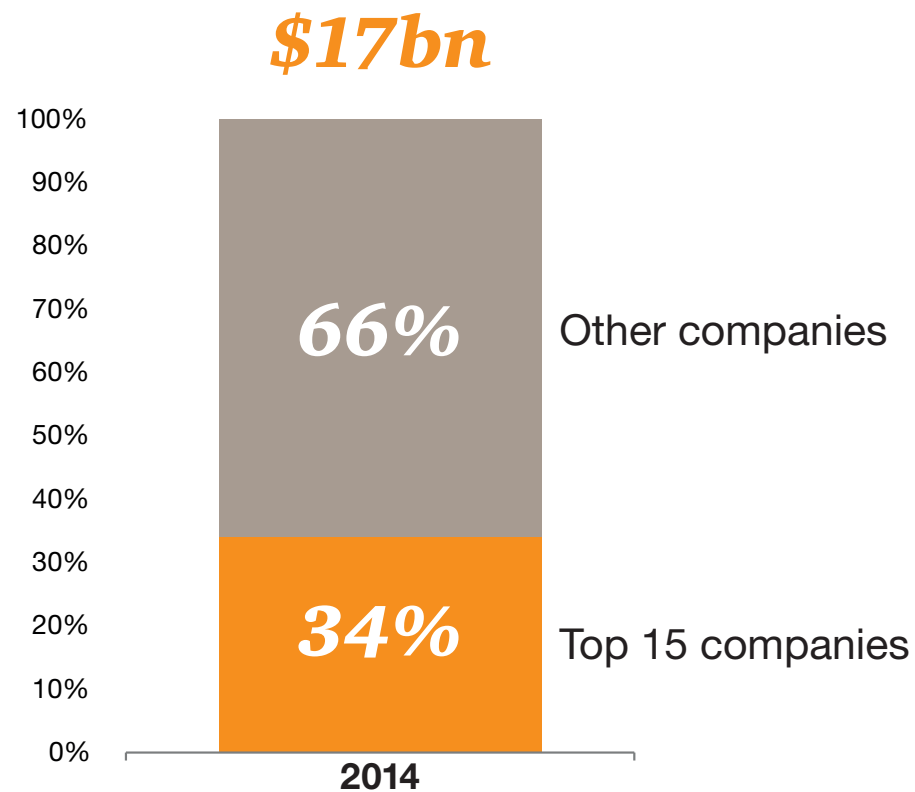
The base of such European cyber security-focused VARs is currently very fragmented, with the **top 15 players** accounting for **just one-third of the market**, with the **remaining two-thirds** comprising a **'long tail'** of other service providers.

While historically these security-focused VARs have been well placed to serve local needs, the majority have not significantly extended the breadth of their capabilities (i.e. beyond basic product resale and implementation) or coverage (i.e. beyond smaller-sized businesses).

An **opportunity exists** to fill this demand gap via a mix of organic growth and M&A, notably by:

- Supplementing security services offerings to include **managed security services** and;
- Selling to increasingly **large customers** (including on a **pan-European basis** more akin to SIs or Telecom operators)

Estimated share of Cyber security market, Western Europe, 2014

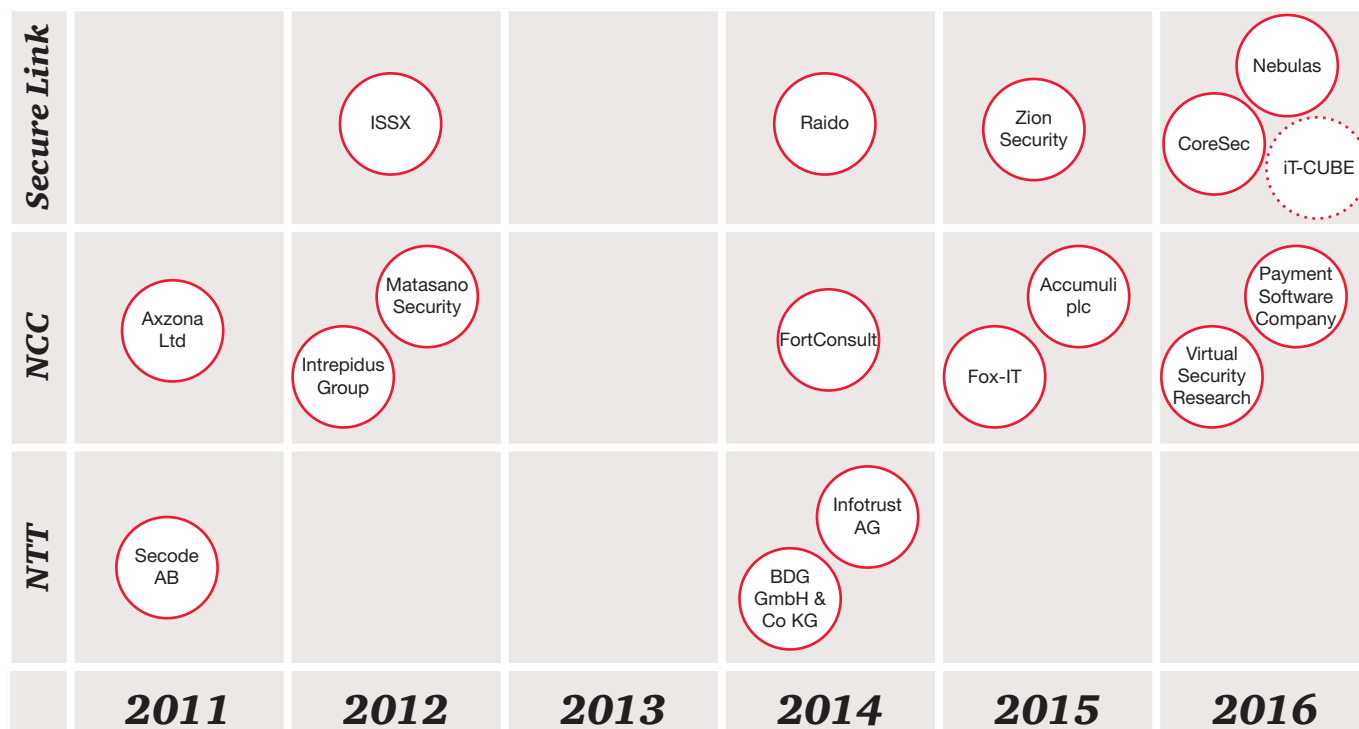


Source: Company reports, PwC survey, IDC, Gartner

Emerging market leaders

There are already some compelling initial proof-points of several security-focused VARs seizing this opportunity and gaining scale and reach: notably, NTT Com Security, NCC and SecureLink.

Acquisition timeline for selected providers



Source: Company websites, Mergermarket

Note: NCC and SecureLink 2016 acquisitions are not included in the revenues shown on p.12, which relate to FY 2015 only; Securelink iT-CUBE acquisition agreed in 2016 but completed January 2017

Through scale, these providers are able to **better meet customer needs** and at the same time **operate more efficiently** (therefore assuring long-term service provision through financial stability).

Better meeting customer needs



8 out of 10 buyers surveyed see value in more pan-European service providers

Source: PwC cyber security buyer survey

Driving cost efficiencies



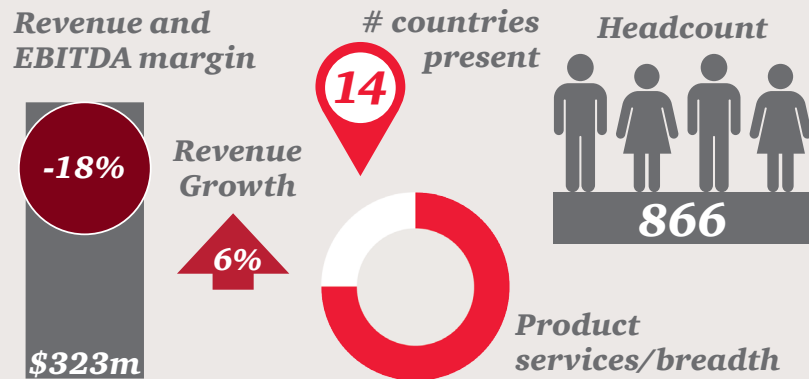
Buying consolidation – opportunity to optimise selected negotiated rates across portfolio of acquired businesses as well as renegotiate on the basis of increased volumes



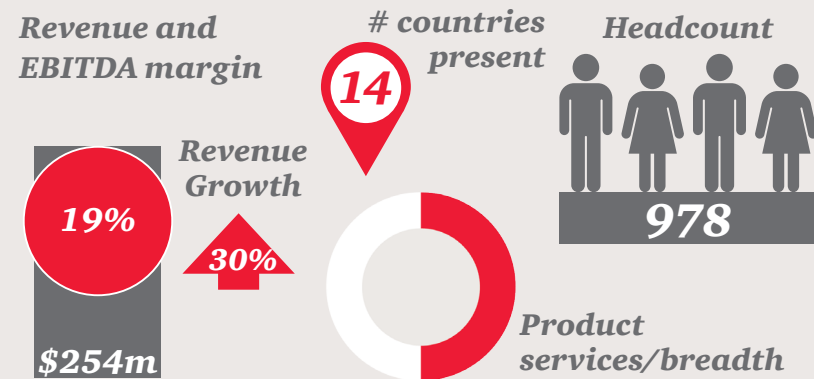
Back office simplification – scope for systems rationalisation, such as providing support/ services to more customers across Europe from a select number of distributed security operations centres (SOC), as well as back-office rationalisation (e.g. finance)

The breadth of geographical and product/service coverage (including provision of more complex managed security services) of these three providers is visible relative to their fragmented peer set and a source of competitive advantage. **NCC and SecureLink, in particular, have outperformed the market to become the two largest independent European service providers, smaller only than NTT-owned NTT Com Security.**

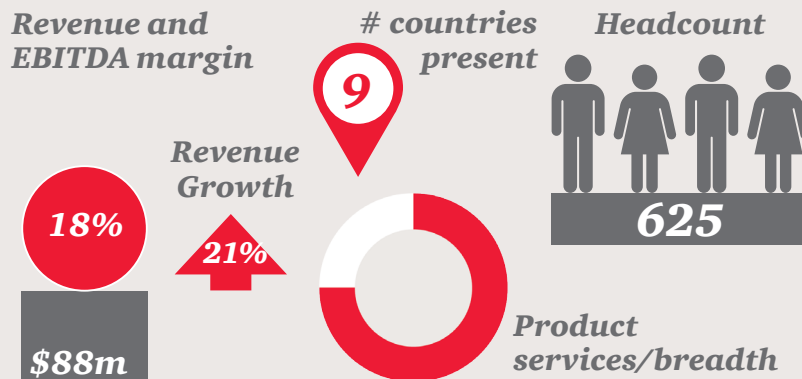
NTT Com Security



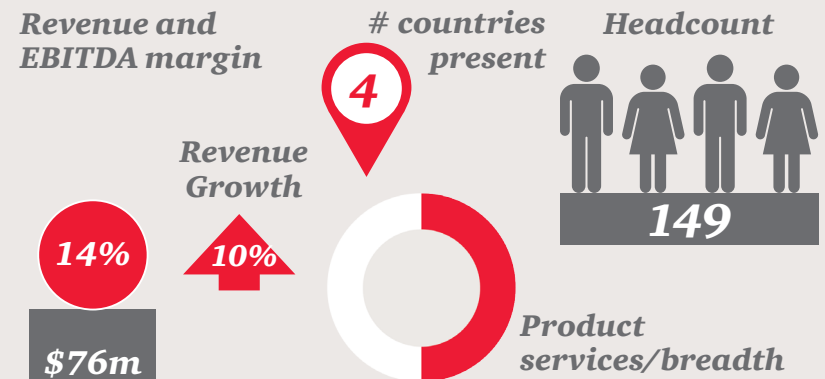
NCC (security division only)



SecureLink



Santa Monica Networks



Source: Company websites, Orbis, Companies House
 Note: All revenues relate to FY2015 with the exception of Voquz which relates to FY2014;
 Revenue growth presented is for last 5 years available with the exception of DCI for whom
 14-15 YOY growth is taken. All other information is latest available from public sources at
 the time of publication.

DCI

Revenue and
EBITDA margin

countries
present

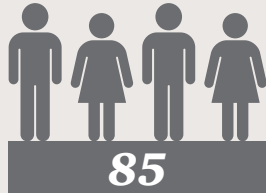
Headcount

13%
\$52m

Revenue
Growth
-18%



Product
services/breadth



SecureData

Revenue and
EBITDA margin

countries
present

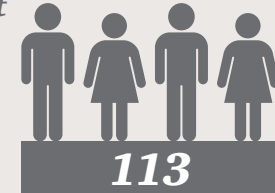
Headcount

8%
\$47m

Revenue
Growth
17%



Product
services/breadth



Voquz

Revenue and
EBITDA margin

countries
present

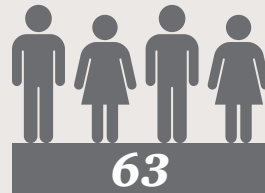
Headcount

2%
\$40m

Revenue
Growth
12%



Product
services/breadth



Open Systems

Revenue and
EBITDA margin

countries
present

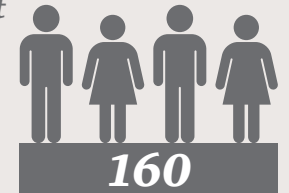
Headcount

EBITDA n/a
\$38m

Revenue
Growth
17%



Product
services/breadth



*The cyber security industry is responding to the increasingly complex cyber threat environment in which organisations now find themselves. **Service providers such as NTT, NCC and SecureLink are early frontrunners, proof of the ability of security-focussed service providers to grow beyond specific local markets through a mix of organic growth and M&A.***

These specialist providers appear well positioned to be able to meet customer needs, while operating in a way that provides comfort around their long-term financial stability (and indeed growth) going forward.

Contacts

Barry Jaber

Partner, UK Technology Industry
Strategy Leader

Tel: +44 (0)20 7213 3522





At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/uk.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2017 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

161228-103409-BM-UK